

PATENT ABSTRACTS OF JAPAN

(1f) Publication number : 2001-274788

(43) Date of publication of application : 05.10.2001

(51)Int.Cl.

H04L 9/08

G06F 13/00

G09C 1/00

H04L 12/18

(21)Application number : 2001-011996

(71)Applicant : INTERNATL BUSINESS MACH CORP <IBM>

(22)Date of filing : 19.01.2001

(72)Inventor : MOURAD MAGDA
MUNSON JONATHAN P
PACIFICI GIOVANNI
TANTAWY AHMED
YOUSSEF ALAA S

(30)Priority

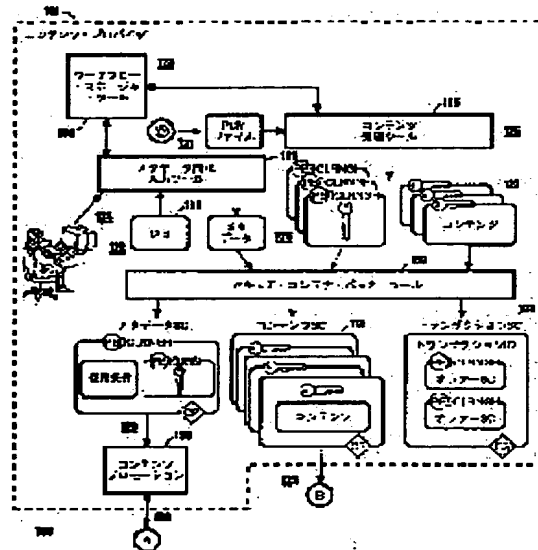
Priority number : 2000 487417 Priority date : 20.01.2000 Priority country : US

(54) DISTRIBUTION OF DIGITAL CONTENTS USING WEB BROADCAST COMMUNICATION SERVICE

(57)Abstract:

PROBLEM TO BE SOLVED: To provide users with a method for surely receiving data on a system from a web broadcast communication interface through a plurality of channels.

SOLUTION: This method includes a step, where promotion meta data that are available for reception are received through a 1st web broadcast communication channel and at least part of the data is assembled into promotion offering data, a step where data to be received are selected in relation to the above data, a step where data are received from a 2nd web broadcast communication channel, a step where the data are selected from the promotion meta data and encrypted by using a 1st encryption key, and a step where a computer-readable medium receives a 1st encryption decoding key, and the decoding key is used to decode at least part of the encrypted data received from the 2nd web broadcast communication channel.



LEGAL STATUS

[Date of request for examination]

19.01.2001

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision]

BEST AVAILABLE COPY

【特許請求の範囲】

【請求項1】複数のチャネルを備えたウェブ同報通信インフラストラクチャによりユーザのシステムに確実にデータを提供する方法であって、

第1の暗号化キーを使用してデータを暗号化するステップと、

第2の暗号化キーを使用して第1の暗号化解除キーを暗号化するステップと、

少なくともユーザのシステム上で受信するために第1のウェブ同報通信チャネル上で暗号化データの少なくとも一部に関連するプロモーション・メタデータを同報通信するステップと、

第2の同報通信チャネルにより暗号化データの少なくとも一部を同報通信するステップと、

暗号化した第1の暗号化解除キーをコンピュータ可読媒体によりユーザのシステムに転送するステップであって、その暗号化した第1の暗号化解除キーが第2の暗号化キーによって暗号化されているステップとを含む方法。

【請求項2】プロモーション・メタデータを同報通信するステップが、所定の時間間隔で定期的にプロモーション・メタデータを同報通信することを含む、請求項1に記載の方法。

【請求項3】プロモーション・メタデータを同報通信するステップが、

少なくともプロモーション・メタデータをウェブ・ブラウザにより読取り可能なフォーマットに変換するサブステップを含む、請求項1に記載の方法。

【請求項4】暗号化データの少なくとも一部を同報通信するステップが、暗号化データの少なくとも一部に関する同報通信時間およびウェブ同報通信チャネルのスケジュールを同報通信することを含む、請求項1に記載の方法。

【請求項5】第2のウェブ同報通信チャネルにより暗号化データの少なくとも一部を同報通信するステップが、DirecPCTMと互換性のあるフォーマットで暗号化データを同報通信することを含む、請求項1に記載の方法。

【請求項6】プロモーション・メタデータがそのデータに関する同報通信時間のスケジュールを含む、請求項1に記載の方法。

【請求項7】複数のチャネルによりウェブ同報通信インフラストラクチャからユーザのシステム上で確実にデータを受信する方法であって、

第1のウェブ同報通信チャネルからプロモーション・メタデータを受信するステップであって、そのプロモーション・メタデータが受信用に使用可能なデータに関するメタ・データであるステップと、

プロモーション・メタデータの少なくとも一部をユーザによる検討用のプロモーション・オフファリングにアセンブルするステップと、

プロモーション・メタデータに関連して受信すべきデータをユーザによって選択するステップと、

第2のウェブ同報通信チャネルからデータを受信するステップであって、そのデータがプロモーション・メタデータから選択されたデータであり、そのデータが第1の暗号化キーを使用してあらかじめ暗号化されているステップと、

コンピュータ可読媒体により第1の暗号化解除キーを受信するステップであって、その第1の暗号化解除キーが第2のウェブ同報通信チャネルにより受信したデータの少なくとも一部を暗号化解除するキーであるステップとを含む方法。

【請求項8】プロモーション・データの少なくとも一部をアセンブルするステップが、プロモーション・データの少なくとも一部をウェブ・ブラウザにより読取り可能なフォーマットにアセンブルすることを含み、選択するステップが、ウェブ・ブラウザにより選択することを含む、請求項7に記載の方法。

【請求項9】選択するステップが、ユーザのシステム上であらかじめ受信され記憶されたプロモーション素材を選択することを含む、請求項7に記載の方法。

【請求項10】選択するステップが、選択したデータの次のウェブ同報通信に関するスケジュールを決定するサブステップと、

ユーザのシステムを起動して第2のチャネル上で次のウェブ同報通信を受信するトリガを設定するサブステップとをさらに含む、請求項9に記載の方法。

【請求項11】第2のウェブ同報通信チャネルからデータを受信するステップが、トリガによって提供されたウェブ同報通信チャネルおよび時間においてプロモーション・メタデータから選択したデータを受信することを含む、請求項10に記載の方法。

【請求項12】第2のウェブ同報通信チャネルからデータを受信するステップが、DirecPCTMと互換性のあるフォーマットでデータを受信することを含む、請求項7に記載の方法。

【請求項13】第2のウェブ同報通信チャネルからデータを受信するステップが、ユーザのシステムが選択したデータを受信することを許可されていることをバック・チャネルにより認可するサブステップを含み、第1の暗号化解除キーを受信するステップが、ユーザのシステムが選択したデータを受信することを許可されている場合にのみ第1の暗号化解除キーを受信することを含む、請求項7に記載の方法。

【請求項14】第2のウェブ同報通信チャネルからデータを受信するステップが、プロモーション・メタデータから選択したデータがユーザのシステム上で受信された場合に、次にユーザがユーザのシステムを起動するときにユーザに状況を通知するサブステップをさらに含む、請求項7に記載の方法。

【請求項15】第1の暗号化解除キーを受信するステップが、第2の暗号化キーにより暗号化された第1の暗号化解除キーを受信することを含む、請求項7に記載の方法。

【請求項16】第1の暗号化解除キーを受信するステップが、同報通信ストリームにより第1の暗号化解除キーを受信することを含む、請求項15に記載の方法。

【請求項17】第2の暗号化解除キーがクリアリングハウスからユーザのシステムに送信される、請求項15に記載の方法。

【請求項18】第2の暗号化解除キーが、クリアリングハウスからユーザのシステムに送信された第2の暗号化キーにより暗号化されたデータを暗号化解除するタイムアウト設備を有する、請求項15に記載の方法。

【請求項19】複数のチャネルを備えたウェブ同報通信インフラストラクチャによりユーザのシステムに確実にデータを提供するシステムであって、コンテンツ・システムと、

第1の公開キーと、

第1の公開キーに対応する第1の秘密キーと、

データ暗号化キーと、

データ暗号化キーを使用して暗号化したデータを暗号化解除するデータ暗号化解除キーと、

データ暗号化解除キーのみによって暗号化解除可能になるようにデータを暗号化する第1のデータ暗号化手段と、

データ暗号化解除キーを暗号化するために第1の公開キーを使用する第2のデータ暗号化手段と、

クリアリング・ハウスと、

第2のウェブ同報通信チャネル上で同報通信されるデータに関連するプロモーション・データを第1のウェブ同報通信チャネル上の1つまたは複数のユーザのシステムに同報通信し、データ暗号化キーにより暗号化したデータを第2の同報通信チャネル上で同報通信する同報通信センタと、

暗号化されたデータ暗号化解除キーをクリアリング・ハウスに転送する第1の転送手段であって、クリアリング・ハウスが第1の秘密キーを所有する第1の転送手段と、

第1の秘密キーを使用してデータ暗号化解除キーを暗号化解除する第1の暗号化解除手段と、

第2の公開キーと、

第2の公開キーに対応する第2の秘密キーと、

第2の公開キーを使用してデータ暗号化解除キーを再暗号化する再暗号化手段と、

再暗号化されたデータ暗号化解除キーをユーザのシステムに転送する第2の転送手段であって、ユーザのシステムが第2の秘密キーを所有する第2の転送手段と、

第2の秘密キーを使用して再暗号化したデータ暗号化解除キーを暗号化解除する第2の暗号化解除手段とを含む

システム。

【請求項20】プロモーション・メタデータがそのデータに関する同報通信時間のスケジュールを含む、請求項19に記載のシステム。

【請求項21】複数のチャネルによりウェブ同報通信インフラストラクチャから確実にデータを受信する、ユーザのシステムであって、

第1のウェブ同報通信チャネルからプロモーション・メタデータを受信する受信機であって、そのプロモーション・メタデータが受信用に使用可能なデータに関するメタデータである受信機と、

プロモーション・メタデータの少なくとも一部をユーザによる検討用に提示する出力装置へのインタフェースと、

プロモーション・メタデータに関連して受信すべきデータに関するユーザによる選択を受信する入力装置へのインタフェースと、

第2のウェブ同報通信チャネルからデータを受信するよう受信機を制御する制御装置であって、そのデータがプロモーション・メタデータから選択されたデータであり、そのデータが第1の暗号化キーを使用してあらかじめ暗号化されている制御装置と、

コンピュータ可読媒体により第1の暗号化解除キーを受信するインタフェースであって、その第1の暗号化解除キーが第2のウェブ同報通信チャネルにより受信したデータの少なくとも一部を暗号化解除するキーであるインタフェースとを含むユーザのシステム。

【請求項22】出力装置がウェブ・ブラウザであり、入力装置がユーザによる選択を受信するためにウェブ・ブラウザに結合されている、請求項21に記載のユーザのシステム。

【請求項23】制御装置が、プロモーション・メタデータから導出したスケジュールであって、第2のウェブ同報通信チャネルからデータを受信するよう受信機を制御するために使用するスケジュールをさらに含む、請求項21に記載のユーザのシステム。

【請求項24】受信機が、DirecPCTMと互換性のあるフォーマットで同報通信されたデータを受信するよう適合されている、請求項21に記載のユーザのシステム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】開示する本発明は、概してエレクトロニック・コマースの分野に関し、より詳細には、インターネット、ワールド・ワイド・ウェブ、ケーブルまたは衛星ディジタル放送網などのグローバル通信ネットワークによる印刷媒体、フィルム、ゲーム、音楽などのデジタル資産の安全な送達および権利管理のためのシステムおよび関連ツールに関する。

【0002】

【従来の技術】音楽、フィルム、コンピュータ・プログ

ラム、ピクチャ、ゲーム、その他のコンテンツなどのデジタル資産の配布のためのインターネットなどのグローバル配布システムの使用は増大し続けている。同時に、貴重なデジタル・コンテンツのオーナーまたは発行者は、いくつかの理由により、デジタル資産の配布のためのインターネットの使用になかなか取り組めなかった。理由の1つは、オーナーがデジタル・コンテンツの無許可コピーまたは海賊版作成を懸念していることである。デジタル・コンテンツの電子送達により、海賊版作成に対するいくつかのバリアが取り除かれる。電子配布によって取り除かれるバリアの1つは、有形の記録可能媒体そのもの（たとえば、ディスクまたはCD-ROM）が必要なことである。多くの場合、ブランク・テープまたは記録可能CDは1ドル未満であっても、デジタル・コンテンツを有形媒体にコピーするには、お金が必要である。しかし、電子配布の場合、有形媒体はもはや不要である。コンテンツは電子的に配布されるので、有形媒体のコストは要因ではなくなる。第2のバリアはコンテンツ自体のフォーマットであり、すなわち、コンテンツは、デジタル・フォーマットではなくアナログ・フォーマットで記憶されている。アナログ・フォーマットで記憶されたコンテンツ、たとえば、印刷ピクチャは、写真複写によって複製したときに、そのコピーはオリジナルより品質が悪くなる。コピーのその後の各コピーは、生成と呼ばれることもあり、コピーのたびにオリジナルより品質が悪くなる。ピクチャがデジタルで記憶されると、このような品質の劣化は存在しない。各コピーならびにどのコピー生成も、オリジナルと同様に鮮明かつ明解なものになりうる。デジタル・コピーが完璧であることと、コンテンツを電子式に配布し、インターネットにより広範囲にコンテンツを配布するためのコストが非常に低いことを結合した集合効果により、無許可コピーの海賊版を作成して配布することは比較的容易になる。数回のキーストロークによって、著作権侵害者は、デジタル・コンテンツの数百部または数千部の完璧なコピーをインターネットにより送信することができる。したがって、電子式に配布されるデジタル資産の保護およびセキュリティを保証することが必要である。

【0003】デジタル・コンテンツのプロバイダは、コンテンツ・オーナーの権利を保護する、デジタル・コンテンツ用の安全なグローバル配布システムの確立を希望している。デジタル・コンテンツ配布システムの確立に関する問題としては、デジタル・コンテンツ電子配布、権利管理、資産保護のためのシステムの開発を含む。電子式に配布されるデジタル・コンテンツは、印刷媒体、フィルム、ゲーム、プログラム、テレビ、マルチメディア、音楽などのコンテンツを含む。

【0004】電子配布システムの配備によって、デジタル・コンテンツ・プロバイダは、即時販売報告および

電子調停により支払の迅速決済を達成すると同時にコンテンツの再配布により2次財源を獲得する能力がもたらされる。電子デジタル・コンテンツ配布システムは物理的な在庫の目減りまたは返品によって左右されないで、デジタル・コンテンツ・プロバイダおよび小売業者は、コストの低減とマージンの改善を実現することができる。デジタル・コンテンツ・プロバイダは、在庫の時限リリースの向上のために新しい流通経路を促進するかまたは既存の流通経路を増強することができる。電子配布システムからのトランザクション・データを使用して、消費者の購入パターンに関する情報を入手すると同時に電子マーケティング・プログラムおよびプロモーションに関する即時フィードバックを提供することができる。これらの目標を満たすために、デジタル資産の保護および計量を保証しながら、デジタル・コンテンツが電子配布モデルを使用して広範囲のユーザおよびビジネスに対してデジタル・コンテンツを使用可能にする必要がある。

【0005】リアル・オーディオ、AT&TによるA2B、Liquid Audio Pro Corp.によるLiquid Audio Pro、Audio SoftによるCity Music Networkなど、デジタル・コンテンツ用のその他の市販の電子配布システムは、保護付きおよび無保護の電子ネットワークによるデジタル・データの伝送を提供する。保護付き電子ネットワークを使用すると、デジタル・コンテンツ・プロバイダの、広範囲の視聴者にデジタルを配布する要件が大幅に低減される。インターネットおよびウェブなどの無保護ネットワークを使用すると、デジタル・コンテンツは暗号化の使用などにより確実にエンドユーザに到着することができる。しかし、暗号化されたデジタル・コンテンツがエンドユーザのマシン上で暗号化解除されると、そのデジタル・コンテンツは無許可再配布のためにエンドユーザにとって容易に使用可能なものになる。したがって、デジタル資産の保護を提供し、デジタル・コンテンツが消費者およびビジネスに送達された後もコンテンツ・プロバイダの権利が保護される、安全なデジタル・コンテンツ電子配布システムが必要になる。したがって、デジタル資産の安全な送達、ライセンス許可、および使用制御を可能にするための権利管理が必要になる。

【0006】デジタル・コンテンツのオーナーが電子配布になかなか取り組めなかったもう1つの理由は、既存の流通経路を維持し育成したいという彼らの希望である。ほとんどのコンテンツ・オーナーは小売業者を通して販売している。音楽市場では、このような米国小売業者としては、Tower Records、Peaches、Blockbuster、Circuit Cityなどを含む。これらの小売業者の多くは、インターネット・ユーザがインターネットによって選択を行い、選択したものをエンドユーザに郵送できるようにするウェブ・サイトを有している。音楽ウェブ・サイトの

例としては、Tower、Music Boulevard、Columbia Houseを含む。電子配布を使用すると、特にウェブ上で、小売店同士が互いに区別し、小売店とコンテンツ・オーナーとを区別する能力が取り除かれる可能性がある。したがって、ピクチャ、ゲーム、音楽、プログラム、ビデオなどの電子コンテンツの小売業者にに対し、電子配布により音楽を販売するときに互いに区別し、小売業者とコンテンツ・オーナーとを区別する方法を提供することが必要である。

【0007】コンテンツ・オーナーは、電子ストアなどの配布サイトからの電子配布用としてそれぞれのデジタル・コンテンツを作成する。インターネット上または他のオンライン・サービスによる電子ストアは、それぞれの製品オフリングおよび製品プロモーションによってストア同士を互いに区別したいと望んでいる。伝統的な店、すなわち、電子ストアに類似した非電子非オンラインの店では、製品プロモーション、製品販売、製品サンプル、自由返品方針、その他のプロモーション・プログラムを使用して、自分の店とその競合店とを区別している。しかし、コンテンツ・プロバイダがデジタル・コンテンツに使用条件を課しているオンライン世界では、電子ストアがストア同士を区別する能力は厳格に制限される場合がある。そのうえ、使用条件を変更できる場合でも、電子ストアは、電子的に製品をプロモートし販売するためにコンテンツ・プロバイダからのデジタル・コンテンツに関連するメタデータを処理するという困難な課題に直面している。電子ストアは、メタデータを処理するときにいくつかの要件を管理する必要がある。第1に、電子ストアは、コンテンツ・プロバイダからのデジタル・コンテンツに関連するメタデータを受信しなければならない。多くの場合、このメタデータの部分部分を暗号化して送信することができ、したがって、コンテンツ・プロバイダは暗号化コンテンツを暗号化解除するためのメカニズムを作成しなければならない。第2に、電子ストアは、そのコンテンツに関する製品マーケティング、製品のポジショニング、その他のプロモーション上の考慮事項を支援するために、コンテンツ・プロバイダからコンテンツを受信する前または電子ストアがコンテンツを受信した後のいずれかに、コンテンツ・プロバイダからのメタデータをあらかじめ見ておきたいと希望する場合がある。第3に、電子ストアは、グラフィックおよびアーティスト情報などのプロモーション素材に使用する所与のメタデータを抽出しなければならない。多くの場合、このプロモーション素材は、そのオンライン・プロモーションで電子ストアが直接使用する。第4に、電子ストアは、許可された使用条件の一部を変更してデジタル・コンテンツの各種オフリングを作成することにより、ストア同士を互いに区別したいと希望する場合がある。第5に、電子ストアは、支払決済のために電子ストアを通り抜ける必要なしに購入者によって自

動的に会計調停ハウスに支払調停を指示するためにURLなどの所与のアドレスをメタデータに挿入するかまたは変更しなければならない場合もある。第6に、電子ストアは、使用条件と一致する、著作権で保護されたデジタル・コンテンツの許可された使用に関するライセンスを作成することが必要になる場合もある。たとえば、このライセンスでは、デジタル・コンテンツの限られた数のコピーを作成するための許可を授与することができる。授与される許可の条件を反映するためにライセンスが必要である。

【0008】これらすべての要件を考慮すると、デジタル・コンテンツに関連するメタデータを処理するために、多くの電子ストアでは、これらの要件を処理するためのカスタマイズ・ソフトウェア・プログラムを作成する。このようなカスタマイズ・ソフトウェア・プログラムを作成するために必要な時間、コスト、およびテストは多大なものになる可能性がある。したがって、このような要件の解決策を提供することが必要である。

【0009】さらに、デジタル・コンテンツのオーナーが電子配布になかなか取り組めなかったもう1つの理由は、電子配布用のコンテンツの作成が難しいことである。今日、多くのコンテンツ・プロバイダは、そのポートフォリオに数千または数万タイトルを有している。音楽の例では、同時に数通りのフォーマット（たとえば、CD、テープ、ミニディスク）で使用可能な単一マスタ録音をコンテンツ・オーナーが有していることは珍しいことではない。そのうえ、単一フォーマットは、特定の流通経路用にマスタを新たに作成したかまたはリミックスしたマスタ録音を有する可能性もある。一例として、ラジオ放送用のミキシングはダンス・クラブのサウンド・トラック用のミキシングとは異なる場合があり、ダンス・クラブのサウンド・トラックは一般に使用可能な消費者用CDとは異なる場合がある。このような様々なミキシングの目録を作成し、追跡することは厄介なものになる可能性がある。しかも、マスタ録音の多くのオーナーは、「ベスト盤」など様々な後続コレクションまたは映画に合わせた音楽サウンド・トラックの編集物、その他のコレクションまたは編集物で古い録音を再発行する場合が多い。デジタルで提供されるコンテンツが増えるにつれて、電子配布用のコンテンツをリミックスし、コード化する必要性が増大する。多くの場合、プロバイダは、正しいマスタ録音を選択するためのガイドとして古い記録フォーマットを使用し、電子配布用のリリースのためにこれらの録音を再処理しコード化させる必要がある。これは、特に、その古いフォーマットを使用して電子配布のために古い録音をリリースし直すのを支援したいと希望するコンテンツ・プロバイダに当てはまる可能性がある。プロバイダは、データベースを調べてタイトル、アーティスト、録音を突き合わせ、コード化パラメータを設定することになる。記録ポートフォリオを求めて

データベースを手動でサーチするこのプロセスは、欠点がないわけではない。1つの欠点は、オペレータが手動でデータベースをサーチして、処理パラメータを適切にセットする必要があることである。もう1つの欠点は、データベースからデータを選択する際にオペレータの転記エラーが発生する可能性があることである。したがって、音声などのコンテンツに関する関連データおよびマスタ記録を自動的に検索するための方法をコンテンツ・プロバイダに提供することが必要である。

【0010】コンテンツ・オーナーは、コード化として知られるプロセスにより、電子配布用のデジタル・コンテンツを作成する。コード化は、コンテンツを取得することと、そのコンテンツがアナログ・フォーマットで提示されている場合はそれをデジタル化することと、さらにそれを圧縮することを含む。伝送または記憶されるデータの量が低減されるので、圧縮するプロセスにより、デジタル・コンテンツはネットワークによって転送することができ、より効率よく記録可能媒体に記憶することができる。しかし、圧縮には欠点がないわけではない。ほとんどの圧縮は何らかの情報の損失を伴い、損失圧縮と呼ばれる。コンテンツ・プロバイダは、どの圧縮アルゴリズムを使用するかと、必要な圧縮レベルを決定しなければならない。たとえば、音楽では、デジタル・コンテンツまたはデジタル歌曲は、音楽のジャンルに応じて非常に異なる特性を有する可能性がある。あるジャンルについて選択された圧縮アルゴリズムおよび圧縮レベルは、他のジャンルの音楽には最適な選択ではない可能性がある。また、コンテンツ・プロバイダは、圧縮・アルゴリズムと圧縮レベルの所与の組合せがあるジャンルの音楽、たとえばクラシックには非常にうまく機能するが、ヘビー・メタルなどの他のジャンルの音楽には不満足な結果をもたらすことに気づく可能性がある。そのうえ、オーディオ・エンジニアは、音楽を等化し、ダイナミック・レンジ調整を実行し、他の前処理および処理設定を実行して、コード化した音楽のジャンルが所望の結果をもたらすことを保証しなければならない。各デジタル・コンテンツごとの等化レベルおよびダイナミック・レンジ設定など、これらのコード化パラメータをいつも手動で設定しなければならないという要件は、厄介なものになる可能性がある。音楽の例に戻ると、様々な音楽ジャンルをカバーするコレクションを伴う音楽のコンテンツ・プロバイダは、コード化すべき各歌曲または各歌曲セットごとにコード化パラメータの所望の組合せを手動で選択しなければならないだろう。したがって、コード化のためのプロセス・パラメータの手動選択の必要性を克服することが必要である。

【0011】

【発明が解決しようとする課題】コンテンツを圧縮するためのプロセスは、特に長篇特作映画などの大型コンテンツ項目の場合、大量の専用計算リソースを必要とする

可能性がある。圧縮アルゴリズムのプロバイダは、自身の圧縮技法に関連する様々な兼ね合いおよび利点を提示している。これらの兼ね合いとしては、コンテンツを圧縮するために必要な時間および計算リソースの量、元のコンテンツから達成される圧縮の量、再生のための所望のビット伝送速度、圧縮したコンテンツのパフォーマンス品質、その他の要因を含む。入力としてマルチメディア・ファイルを取り入れ、コード化した出力ファイルを生成し、経過および状況の中間表示を一切行わないコード化プログラムを使用することは問題である。しかも、多くの状況では、経過の中間表示を一切行わないコード化プログラムを呼び出すかまたはそれを管理するために、他のプログラムを使用する。このため、呼出しアプリケーションには、コード化すべきものとして指定された選択内容全体のパーセンテージとして、コード化されたコンテンツの量を測定する方法は一切残されない。呼出しプログラムが一度に実行するよう数通りのプログラムをスケジューリングしようと試みる状況では、これは問題になる可能性がある。さらに、コード化のためにコンテンツ・バッチが選択され、コンテンツ・プロバイダがコード化プロセスの経過を判定したいと希望する場合、これは特に厄介なものになる可能性がある。したがって、このような問題を克服することが必要である。

【0012】デジタル・コンテンツ・プロバイダが自身のコンテンツのために電子配布をなかなか採用しなかったさらにもう1つの理由は、電子的に送達されたコンテンツ用としてエンドユーザ装置上のデジタル・プレーヤを作成するための標準がなかったことである。コンテンツ・プロバイダ、電子ストア、電子配布チェーン内のその他のものは、PC、セットトップ・ボックス、ハンドヘルド装置などの様々な装置上でカスタマイズ・プレーヤを提供したいと希望している可能性がある。改竄防止環境、すなわち、第三者による再生中にコンテンツへの無許可アクセスを阻止するための環境でデジタル・コンテンツの暗号化解除を処理できる1組のツールが必要である。そのうえ、購入したもの以外の用途でエンド・ユーザがコンテンツにアクセスできないようにして、エンド・ユーザがデジタル・コンテンツのローカル・ライブラリを管理できるようにする1組のツールが必要である。

【0013】デジタル・コンテンツ・プロバイダがデジタル・コンテンツのオンライン配布をなかなか採用しなかったさらにもう1つの理由は、圧縮済みであってもコンテンツを標準の電話回線によって送達するために要する時間である。既存の同報通信インフラストラクチャによりデジタル・コンテンツのダウンロードを可能にする、Intel Intellicastシステムや「Hughes DirecPC」など、同報通信インフラストラクチャにより情報を提供するのためのその他のシステムが存在する。これらの同報通信システムは、有用ではあるが、欠点がないわけ

ではない。まず初めに、これらのシステムは、デジタル・コンテンツの配布のために安全な環境を提供しない。今日使用可能なシステムの多くは、所望のデジタル・コンテンツを選択するために、通常は電話回線であるバック・チャネルを使用する必要がある。バック・チャネルまたは電話回線が使用不能である場合、そのコンテンツは選択することができない。その他のシステムは、単一デジタル・チャネルでプロモーション・データ、コンテンツ・データ、メタデータを提供するわけではなく、むしろ、これらの機能の1つまたは複数のために追加の両方向チャネルを必要とする。本発明では、ダウンロードオンデマンドならびに破壊されたコンテンツ・データ・ブロックの効率の良い再伝送のために、それが使用可能であれば両方向チャネルを使用することができる。したがって、この欠点を克服することが必要である。

【0014】現行同報通信システムのもう1つの欠点は、通信回線、同報通信インフラストラクチャ、DVDおよびCDなどのコンピュータ可読媒体によりコンテンツを確実に配布するためにコンテンツのプロバイダが同一ツールを使用できないことである。したがって、これらの問題を克服するために同報通信インフラストラクチャによりデジタル・コンテンツの送達を可能にするための方法およびシステムが必要である。

【0015】デジタル・コンテンツ保護の背景に関する詳細は、以下の3つの情報源から得られる。<http://www.a2bmusic.com/about/papers/musicipp.htm>というURLでオンラインで入手可能なAT&T Labs (Florham Park, N.J.) のJack Lacy, James Snyder, David Maherによる「Music on the Internet and the Intellectual Property Protection Problem」。<http://www.intertrust.com/architecture/stc.html>というURLでオンラインで入手可能なInterTrust Technologies Corp. (Sunnyvale, CA) のOlin Silbert, David Bernstein, David Van Wijkによる「Securing the Content, Not the Wire for Information Commerce」という記事に記載されたDigiboxという暗号保護コンテナ。<http://cyptolope.ibm.com/white.htm>というURLでオンラインで入手可能な「Cryptolope Container Technology」というIBM White Paper。

【0016】

【課題を解決するための手段】複数のチャネルによりウェブ同報通信インフラストラクチャからユーザのシステム上で確実にデータを受信する方法である。この方法は、第1のウェブ同報通信チャネルからプロモーション・メタデータを受信するステップであって、そのプロモーション・メタデータが受信用に使用可能なデータに関するものであるステップと、プロモーション・メタデータの少なくとも一部をユーザによる検討用のプロモーション・オファリングにアセンブルするステップと、プロ

モーション・メタデータに関連して受信すべきデータをユーザによって選択するステップと、第2のウェブ同報通信チャネルからデータを受信するステップであって、そのデータがプロモーション・メタデータから選択されたものであり、そのデータが第1の暗号化キーを使用してあらかじめ暗号化されているステップと、コンピュータ可読媒体により第1の暗号化解除キーを受信するステップであって、その第1の暗号化解除キーが第2のウェブ同報通信チャネルにより受信したデータの少なくとも一部を暗号化解除するためのものであるステップとを含む。

【0017】他の実施形態では、ウェブ同報通信センタから確実にデータを伝送するための方法およびシステムを開示する。

【0018】

【発明の実施の形態】本実施形態の各項を迅速に突き止めるのを支援するために、本発明に関する目次を示す。

【0019】I. セキュア・デジタル・コンテンツ電子配布システム

40 A. システム概要

1. 権利管理
2. 計量
3. オープン・アーキテクチャ

B. システム機能要素

1. コンテンツ・プロバイダ
2. 電子デジタル・コンテンツ・ストア
3. 中間市場パートナー
4. クリアリング・ハウス
5. エンドユーザ装置
6. 伝送インフラストラクチャ

30 C. システム用途

II. 暗号概念およびセキュア・デジタル・コンテンツ電子配布システムへの応用

- A. 対称アルゴリズム
- B. 公開キー・アルゴリズム
- C. デジタル・シグニチャ
- D. デジタル証書
- E. SC図形表現のガイド
- F. セキュア・コンテナ暗号化の例

40 III. セキュア・デジタル・コンテンツ電子配布システムのフロー

IV. 権利管理アーキテクチャ・モデル

- A. アーキテクチャ層機能
- B. 機能区分およびフロー
 1. コンテンツ・フォーマット層
 2. コンテンツ使用制御層
 3. コンテンツ識別層
 4. ライセンス制御層
- C. コンテンツ配布ライセンス制御
- V. セキュア・コンテナ構造

- A. 一般構造
- B. 権利管理言語構文およびセマンティクス
- C. セキュア・コンテナのフローおよび処理の概要
- D. メタデータ・セキュア・コンテナ620のフォーマット
- E. オフラー・セキュア・コンテナ641のフォーマット
- F. トランザクション・セキュア・コンテナ640のフォーマット
- G. オーダ・セキュア・コンテナ650のフォーマット 10
- H. ライセンス・セキュア・コンテナ660のフォーマット
- I. コンテンツ・セキュア・コンテナのフォーマット
- VI. セキュア・コンテナのバックおよびアンバック
 - A. 概要
 - B. 素材一覧表(BOM) パーツ
 - C. キー記述パーツ
- VII. クリアリング・ハウス
 - A. 概要
 - B. 権利管理処理
 - C. 国別固有パラメータ
 - D. 監査ログおよび追跡
 - E. 結果の報告
 - F. 請求および支払検証
 - G. 再伝送
- VIII. コンテンツ・プロバイダ
 - A. 概要
 - B. ワーク・フロー・マネージャ
 - 1. 製品待受けアクション/情報プロセス
 - 2. 新コンテンツ要求プロセス
 - 3. 自動メタデータ収集プロセス
 - 4. 手動メタデータ入力プロセス
 - 5. 使用条件プロセス
 - 6. 監視付きリリース・プロセス
 - 7. メタデータSC作成プロセス
 - 8. ウォータマーク・プロセス
 - 9. 前処理圧縮プロセス
 - 10. コンテンツ品質管理プロセス
 - 11. 暗号化プロセス
 - 12. コンテンツSC作成プロセス
 - 13. 最終品質保証プロセス
 - 14. コンテンツ分散プロセス
 - 15. ワーク・フロー規則
 - C. メタデータ同化入力ツール
 - 1. 自動メタデータ収集ツール
 - 2. 手動メタデータ入力ツール
 - 3. 使用条件ツール
 - 4. メタデータSCの各パーツ
 - 5. 監視付きリリース・ツール
 - D. コンテンツ処理ツール

- 1. ウォータマーク・ツール
- 2. 前処理圧縮ツール
- 3. コンテンツ品質管理ツール
- 4. 暗号化ツール
- E. コンテンツSC作成ツール
- F. 最終品質保証ツール
- G. コンテンツ分散ツール
- H. コンテンツ・プロモーション・ウェブ・サイト
- I. コンテンツ・ホスト
 - 1. コンテンツ・ホスト・サイト
 - 2. セキュア・デジタル・コンテンツ電子配布システムによって提供されるコンテンツ・ホスト・サイト111
- IX. 電子デジタル・コンテンツ・ストア
 - A. 概要-複数電子デジタル・コンテンツ・ストアのサポート
 - B. ポイントツーポイント電子デジタル・コンテンツ配布サービス
 - 1. 統合要件
- 20 2. コンテンツ収集ツール
- 3. トランザクション処理モジュール
- 4. 通知インタフェース・モジュール
- 5. 会計調停ツール
- C. 同報通信電子デジタル・コンテンツ配布サービス
 - 1. マルチティア・デジタルTVの実施形態
 - 2. 個別チャネルによるウェブ同報通信の実施形態
- X. エンドユーザ装置
 - A. 概要
 - B. アプリケーションのインストール
- 30 C. セキュア・コンテナ・プロセッサ
 - D. プレーヤ・アプリケーション
 - 1. 概要
 - 2. エンドユーザ・インタフェース・コンポーネント
 - 3. コピー/再生管理コンポーネント
 - 4. 暗号化解除1505、圧縮解除1506、再生の各コンポーネント
 - 5. データ管理1502およびライブラリ・アクセスの各コンポーネント
 - 6. アプリケーション間通信コンポーネント
- 40 7. その他の各種コンポーネント
- 8. 汎用プレーヤ
- E. 同報通信送達モードのエンドユーザ装置109
 - 1. マルチティア・デジタルTVの実施形態
- 個別チャネルによるウェブ同報通信の実施形態
- 【0020】I. セキュア・デジタル・コンテンツ電子配布システム
 - A. システム概要
 - セキュア・デジタル・コンテンツ電子配布システムは、エンドユーザ・クライアント装置へのデジタル・
- 50 コンテンツおよびデジタル・コンテンツ関連コンテン

ツの安全な送達および権利管理に必要な技術、仕様、ツール、ソフトウェアを包含する技術プラットフォームである。エンドユーザ装置としては、PC、セット・トップ・ボックス（IRD）、インターネット家電を含む。これらの装置は、コンテンツ所有者によって許可された外部媒体または携帯用消費者装置にそのコンテンツをコピーすることができる。デジタル・コンテンツまたは単にコンテンツという用語は、デジタル・フォーマットで記憶された情報およびデータを意味し、ピクチャ、映画、ビデオ、音楽、プログラム、マルチメディア、ゲームを含む。

【0021】この技術プラットフォームは、どのようにしてデジタル・コンテンツを作成し、エンドユーザ装置にライセンスされたポイントツーポイント・インフラストラクチャおよび同報通信インフラストラクチャ（ケーブル、インターネット、衛星、無線など）により確実に配布し、無許可コピーまたは再生から保護するかを指定するものである。そのうえ、この技術プラットフォームのアーキテクチャは、それらが経時的に進化するにつれて、ウォーターマーク、圧縮／コード化、暗号化、その他のセキュリティ・アルゴリズムなどの様々な技術の統合および移行を可能にする。

【0022】セキュア・デジタル・コンテンツ電子配布システムのベース・コンポーネントは、（1）コンテンツ所有者の所有権の保護のための権利管理と、（2）即時および正確な補償のためのトランザクション計量と、（3）コンテンツ・プロバイダがコンテンツを作成し、任意の規格適合プレーヤで再生するために複数のネットワーク・インフラストラクチャによるその安全な送達を許可できるようにする、オープンかつ文書による十分な裏づけのあるアーキテクチャである。

【0023】1. 権利管理

セキュア・デジタル・コンテンツ電子配布システムにおける権利管理は、システムの動作コンポーネント間に分散された1組の機能によって実施される。その1次機能としては、ライセンスを確保した許可中間ユーザまたはエンドユーザだけがコンテンツをロック解除するようにするライセンス許可および制御と、許可されたコピー数、再生回数、そのライセンスが有効である時間間隔または期間など、購入またはライセンスの条件に応じたコンテンツ使用の制御および執行を含む。権利管理の2次機能は、コンテンツの無許可コピーの発生源を識別するための手段によって著作権侵害と闘えるようにすることである。

【0024】ライセンス許可および制御は、クリアリング・ハウスエンティティとセキュア・コンテナ（SC）技術の使用によって実施される。クリアリング・ハウスは、中間ユーザまたはエンドユーザがライセンス・トランザクションの正常終了を検証した後でコンテンツをロック解除できるようにすることによってライセンス許可

を可能にする。セキュア・コンテナは、暗号化したコンテンツおよび情報をシステム・コンポーネント間に分散するために使用する。SCは、電子情報およびコンテンツに対する無許可インターセプトまたは変更から保護するために暗号化、デジタル・シグニチャ、デジタル証書を使用する情報またはコンテンツの暗号キャリアである。また、これは、デジタル・コンテンツの信憑性および完全性の検証も可能にする。これらの権利管理機能の利点は、デジタル・コンテンツの電子配布インフラストラクチャが安全であるかまたは信頼できるものである必要がないことである。したがって、ウェブおよびインターネットなどのネットワーク・インフラストラクチャによる伝送が可能になる。これは、コンテンツがセキュア・コンテナ内で暗号化され、その記憶および配布がそのロック解除および使用の制御から切り離されているという事実による。暗号化解除キーを有するユーザだけが暗号化コンテンツをロック解除することができ、クリアリング・ハウスは許可された適切な使用要求についてのみ暗号化解除キーをリリースする。クリアリング・ハウスは、未知または無許可の当事者からの偽要求またはコンテンツ所有者が設定したコンテンツの使用条件に適合しない要求をクリアしなくなる。そのうえ、その伝送中にSCが改竄された場合、クリアリング・ハウス内のソフトウェアは、SC内のコンテンツが破壊または変造されたと判断し、そのトランザクションを拒絶する。

【0025】コンテンツの使用制御は、エンドユーザ装置上で実行されるエンドユーザ・プレーヤ・アプリケーション195によって可能になる。このアプリケーションは、2次コピーおよび再生の許容数を定義するデジタル・コードをコンテンツのすべてのコピーに埋め込む。このデジタル・コードを生成し、それを他のエンドユーザ・プレーヤ・アプリケーション195から隠された状態で保持し、それを変更試行に耐えられるものにするために、デジタル・ウォーターマーク技術を使用する。代替実施形態では、このデジタル・コードは、コンテンツ113に関連する使用条件の一部として保持されるだけである。適合エンドユーザ装置内でデジタル・コンテンツ113にアクセスすると、エンドユーザ・プレーヤ・アプリケーション195はそのウォーターマークを読み取って用途制限をチェックし、必要に応じてそのウォーターマークを更新する。要求されたコンテンツの用途が使用条件に適合しない場合、たとえば、コピー数を使い果たしている場合、エンドユーザ装置はその要求を実行しなくなる。

【0026】デジタル・ウォーターマークは、コンテンツの許可コピーまたは無許可コピーの発生源を識別するための手段も提供する。コンテンツ内の初期ウォーターマークは、コンテンツ所有者を識別し、著作権情報を指定し、配布地域を定義し、その他の関連情報を追加するために、コンテンツ所有者によって埋め込まれる。第2の

ウォーターマークは、コンテンツ購入者（またはライセンス保持者）およびエンドユーザ装置を識別し、購入またはライセンス条件および日付を指定し、その他の関連情報を追加するために、エンドユーザ装置側でコンテンツ内に埋め込まれる。

【0027】ウォーターマークはコンテンツの一体部分になるので、コピーが許可されているかどうかとは無関係に、コピーで伝達される。したがって、デジタル・コンテンツは、コンテンツがどこに存在するかまたはどこから来たかにかかわらず、そのソースおよびその許可用途に関する情報を必ず含んでいる。この情報は、コンテンツの違法使用と闘うために使用することができる。

【0028】2. 計量

その権利管理機能の一部として、クリアリング・ハウスは、クリアリング・ハウスによりキー交換がクリアされるすべてのトランザクションを記録する。この記録により、ライセンス許可と元の使用条件の計量が可能になる。トランザクション記録は、取引の支払およびその他の使用の電子調停を容易にするために即時または定期的にコンテンツ所有者またはコンテンツ・プロバイダ、小売業者、その他などの担当当事者に報告することができる。

【0029】3. オープン・アーキテクチャ

セキュア・デジタル・コンテンツ電子配布システム（システム）は、コンテンツ所有者のための権利保護を維持しながら市場におけるシステムの幅広い実施と受入れを容易にするために、仕様書およびインタフェースを備えたオープン・アーキテクチャである。システム・アーキテクチャの柔軟性と開放性により、システムは、様々な技術、伝送インフラストラクチャ、装置が市場に送達されるにつれて、経時的に進化することもできる。

【0030】このアーキテクチャは、コンテンツの性質とそのフォーマットの点ではオープンである。オーディオ、プログラム、マルチメディア、ビデオ、その他のタイプのコンテンツの配布は、このアーキテクチャによってサポートされる。コンテンツは、デジタル音楽用のリニアPCMなどの固有フォーマットか、またはフィルタリング、圧縮、ブリエンファシス／デエンファシスなどの追加の前処理またはコード化によって達成されるフォーマットにすることができるだろう。このアーキテクチャは、様々な暗号化およびウォーターマーク技法によってオープンなものである。これは、様々なコンテンツ・タイプおよびフォーマットに対処し、それらが進化するにつれて新しい技術の導入または採用を可能にするために、特定の技法の選択を可能にする。この柔軟性により、コンテンツ・プロバイダはセキュア・デジタル・コンテンツ電子配布システム内でデータ圧縮、暗号化、およびフォーマットのために使用する技術を選び出し、進化させることができる。

【0031】また、このアーキテクチャは、様々な配布

ネットワークおよび配布モデルにとってもオープンなものである。このアーキテクチャは、低速インターネット接続または高速衛星およびケーブル・ネットワークによるコンテンツ配布をサポートし、ポイントツーポイント・モデルまたは同報通信モデルとともに使用することができる。そのうえ、このアーキテクチャは、低コスト消費者装置を含む多種多様な装置上でエンドユーザ装置内の諸機能を実施できるように設計されている。この柔軟性により、コンテンツ・プロバイダおよび小売業者は多様なサービス・オファリングによって中間ユーザまたはエンドユーザにコンテンツを提供することができ、ユーザはコンテンツを購入またはライセンスし、それを再生し、それを様々な適合プレーヤ装置に記録することができる。

【0032】B. システム機能要素

次に図1ないし図4に移行すると、本発明によるセキュア・デジタル・コンテンツ電子配布システム100の概要を示すブロック図が示されている。セキュア・デジタル・コンテンツ電子配布システム100は、エンドツーエンド・ソリューションを含む複数のビジネス要素を包含し、コンテンツ・プロバイダ（101）またはデジタル・コンテンツの所有者、電子デジタル・コンテンツ・ストア103、中間市場パートナー（図示せず）、クリアリング・ハウス105、コンテンツ・ホスト・サイト111、伝送インフラストラクチャ107、エンドユーザ装置109を含む。これらのビジネス要素のそれぞれは、セキュア・デジタル・コンテンツ電子配布システム100の様々なコンポーネントを使用する。特に電子コンテンツ113の配布に関連するので、これらのビジネス要素とシステム・コンポーネントの高レベルの説明を以下に示す。

【0033】1. コンテンツ・プロバイダ101

コンテンツ・プロバイダ101またはコンテンツ所有者は、元のコンテンツ113のオーナーであるか、またはさらに配布するために独立したコンテンツ113をパッケージ化する権限を授与された配布者あるいはその両方である。コンテンツ・プロバイダ101は、自分の権利を直接活用するか、あるいは通常はエレクトロニック・コマースの収入に関するコンテンツ使用の支払と引き換えに電子デジタル・コンテンツ・ストア103または中間市場パートナー（図示せず）にコンテンツ113をライセンスすることができる。コンテンツ・プロバイダ101の例としては、ソニー、タイムワナー、MTV、IBM、マイクロソフト、ターナー、フォックスなどを含む。

【0034】コンテンツ・プロバイダ101は、配布のために自分のコンテンツ113と関連データを作成するために、セキュア・デジタル・コンテンツ電子配布システム100の一部として提供されたツールを使用する。ワーク・フロー・マネージャ・ツール154は、処

理すべきコンテンツ113をスケジューリングし、高い品質保証を維持するためにコンテンツ113の作成およびパッケージ化の様々なステップを通過するときにコンテンツ113を追跡する。コンテンツ113に関するデータを意味するために本明細書全体を通してメタデータという用語を使用するが、この用語は本実施形態ではコンテンツ113そのものは含まない。一例として、歌曲のメタデータは、歌曲タイトルまたは歌曲クレジットにすることができるが、その歌曲の録音にすることはできない。コンテンツ113は録音を含むことになるだろう。メタデータ同化入力ツール161は、コンテンツ・プロバイダのデータベース160からのメタデータまたは規定のフォーマットでコンテンツ・プロバイダによって提供されるデータ（音楽の例の場合、CDタイトル、アーティスト名、歌曲タイトル、CDアートワークなどのコンテンツ113の情報）を抽出し、電子配布のためにそれをパッケージ化するために使用する。また、メタデータ同化入力ツール161は、コンテンツ113の使用条件を入力するためにも使用する。使用条件のデータとしては、コピー制限規則、卸売価格、必要と思われる任意のビジネス規則を含むことができる。ウォーターマーク・ツールは、コンテンツ・オーナー、処理日、その他の関連データを識別するデータをコンテンツ113内に隠すために使用する。コンテンツ113がオーディオである実施形態の場合、オーディオ・ブリプロセッサ・ツールを使用して、最適圧縮品質のために強弱の変化を調節するかあるいはコンテンツ113またはその他のオーディオを等化し、所望の圧縮レベルまでコンテンツ113を圧縮し、コンテンツ113を暗号化する。これらは、デジタル・コンテンツ圧縮/コード化、暗号化、フォーマット方法の技術的進歩に追従し、市場でそれらが経時的に進化するにつれてコンテンツ・プロバイダ101が最良のツールを使用できるように適合させることができる。

【0035】暗号化コンテンツ113、デジタル・コンテンツ関連データまたはメタデータ、暗号化キーは、SCバック・ツールによってSC（以下に記載する）内にバックされ、電子配布のためにコンテンツ・ホスト・サイトまたはプロモーション・ウェブ・サイトあるいはその両方に記憶される。コンテンツ・ホスト・サイトは、コンテンツ・プロバイダ101に存在するか、あるいは電子デジタル・コンテンツ・ストア103および中間市場パートナー（図示せず）設備を含む複数の位置に存在する可能性がある。コンテンツ113とキー（以下に記載する）はいずれも暗号化され、SC内にバックされるので、電子デジタル・コンテンツ・ストア103または他のホスト・エージェントは、クリアリング・ハウスからのクリアランスとコンテンツ・プロバイダ101への通知なしに、暗号化解除したコンテンツ113に直接アクセスすることはできない。

【0036】2. 電子デジタル・コンテンツ・ストア103

電子デジタル・コンテンツ・ストア103は、コンテンツ113のテーマ・プログラミングまたはコンテンツ113の電子マーチャンドライジングなど多種多様なサービスまたはアプリケーションによりコンテンツ113のマーケティングを行うエンティティである。電子デジタル・コンテンツ・ストア103は、自分のサービスの設計、開発、事業計画、決済、マーチャンドライジング、マーケティング、販売を管理する。オンライン電子デジタル・コンテンツ・ストア103の例は、ソフトウェアの電子ダウンロードを提供するウェブ・サイトである。

【0037】それぞれのサービス内で電子デジタル・コンテンツ・ストア103は、セキュア・デジタル・コンテンツ電子配布システム100の所与の機能を実施する。電子デジタル・コンテンツ・ストア103は、コンテンツ・プロバイダ101からの情報を集め、コンテンツとメタデータを追加のSC内にバックし、サービスまたはアプリケーションの一部としてそのSCを消費者またはビジネスに送達する。電子デジタル・コンテンツ・ストア103は、セキュア・デジタル・コンテンツ電子配布システム100によって提供されるツールを使用して、メタデータ抽出、2次使用条件、SCパッケージ化、電子コンテンツ・トランザクションの追跡を支援する。2次使用条件データとしては、コンテンツ113の購入価格、ペーパーリッスン価格、コピー許可、ターゲット装置タイプ、時限可用性制限などの小売業ビジネス・オファーを含むことができる。

【0038】電子デジタル・コンテンツ・ストア103がエンドユーザからの電子コンテンツ113を求める有効な要求を完了すると、電子デジタル・コンテンツ・ストア103は、顧客にコンテンツ113用の暗号化解除キーをリリースする権限をクリアリング・ハウス105に授与する責任がある。また、電子デジタル・コンテンツ・ストアは、コンテンツ113を含むSCのダウンロードも許可する。電子デジタル・コンテンツ・ストアは、そのローカル・サイト側でデジタル・コンテンツを含むSCをホストとして処理することを選ぶか、あるいは他のコンテンツ・ホスト・サイトのホストおよび配布設備を使用することができる。

【0039】電子デジタル・コンテンツ・ストアは、セキュア・デジタル・コンテンツ電子配布システム100を使用して、エンドユーザが有する可能性のある任意の質問または問題に関する顧客サービスを提供することができるか、あるいは電子デジタル・コンテンツ・ストア103は、その顧客サービス・サポートをクリアリング・ハウス105に外注することもできる。

【0040】3. 中間市場パートナー（図示せず）

代替実施形態では、セキュア・デジタル・コンテンツ

電子配布システム100を使用して、中間市場パートナーと呼ばれる他のビジネスにコンテンツ113を確実に提供することができる。このようなパートナーとしては、コンテンツ113を配布するテレビ局またはビデオ・クラブ、ラジオ放送局またはレコード・クラブなど、非電子サービスを提供するデジタル・コンテンツ関連会社を含むことができる。また、このようなパートナーとしては、レコード・スタジオ、複製業者、生産者など、録音の作成またはマーケティングの一部として素材を扱う他の信頼できる当事者も含むことができる。このような中間市場パートナーは、コンテンツ113を暗号化解除するために、クリアリング・ハウス105からのクリアランスが必要である。

【0041】4. クリアリング・ハウス105

クリアリング・ハウス105は、SC内に暗号化されたコンテンツ113の販売または許可された使用あるいはその両方に関連するすべてのトランザクションに関するライセンス許可および記録保持を行う。クリアリング・ハウス105がコンテンツ113用の暗号化解除キーを求める要求を中間ユーザまたはエンドユーザから受け取ると、クリアリング・ハウス105は、要求内の情報の完全性および信憑性を妥当性検査し、その要求が電子デジタル・コンテンツ・ストアまたはコンテンツ・プロバイダ101によって許可されたことを検証し、要求された使用がコンテンツ・プロバイダ101によって定義されたコンテンツ使用条件に適合することを検証する。このような検証が履行されると、クリアリング・ハウス105はライセンスSCにバックしたコンテンツ113用の暗号化解除キーを要求側エンドユーザに送信する。このキーは、許可ユーザだけがそれを検索できるように暗号化される。エンドユーザの要求が検証不能であるか、不完全であるか、または許可されていない場合、クリアリング・ハウス105は暗号化解除キーを求めるその要求を拒絶する。

【0042】クリアリング・ハウス105は、すべてのトランザクションを記録し、即時、定期的、または制限付きで電子デジタル・コンテンツ・ストア103およびコンテンツ・プロバイダ101などの担当当事者にそれを報告することができる。この報告は、それによりコンテンツ・プロバイダ101にコンテンツ113の販売を通知することができ、電子デジタル・コンテンツ・ストア103がその顧客への電子送達の監査証跡を入手することができる手段である。また、クリアリング・ハウス105は、SC内の情報が損なわれているかまたはコンテンツの使用条件に適合しないことを検出した場合、コンテンツ・プロバイダ101または電子デジタル・コンテンツ・ストア103あるいはその両方に通知することもできる。クリアリング・ハウス105のデータベースのトランザクション記録リポトリ機能は、データ・マイニングまたは報告書作成用に構造化されてい

る。

【0043】他の実施形態では、クリアリング・ハウス105は、償還、伝送障害、購入紛争など、トランザクションに関する顧客サポートおよび例外処理を行うことができる。クリアリング・ハウス105は、権利管理および計量のための信頼できる管理人を提供する独立エンティティとして運営することができる。これは、必要に応じて請求および決済を行う。電子クリアリング・ハウスの例としては、Secure-Bank.comと、ビザ/マスター・カードによるセキュア・エレクトロニック・トランザクション(SET)を含む。一実施形態のクリアリング・ハウス105はエンドユーザ装置109にとってアクセス可能なウェブ・サイトである。他の実施形態のクリアリング・ハウス105は電子デジタル・コンテンツ・ストア103の一部である。

【0044】5. エンドユーザ装置109

エンドユーザ装置109は、セキュア・デジタル・コンテンツ電子配布システム100の仕様に適合するエンドユーザ・プレーヤ・アプリケーション195(後述する)を含む任意のプレーヤ装置にすることができる。このような装置としては、PC、セット・トップ・ボックス(IRD)、インターネット家電を含むことができる。エンドユーザ・プレーヤ・アプリケーション195は、ソフトウェアまたは消費者エレクトロニクス・ハードウェアあるいはその両方で実現することができる。再生、記録、ライブラリ管理の諸機能に加え、エンドユーザ・プレーヤ・アプリケーション195は、エンドユーザ装置109で権利管理を可能にするためのSC処理を行う。エンドユーザ装置109は、デジタル・コンテンツを含むSCのダウンロードおよび記憶を管理し、クリアリング・ハウス105から暗号化デジタル・コンテンツ・キーの受取りを要求して管理し、デジタル・コンテンツをコピーまたは再生するたびにウォーターマークを処理し、デジタル・コンテンツの使用条件に応じて作成したコピー数(またはコピーの削除)を管理し、許されるならば外部媒体または携帯用消費者装置へのコピーを実行する。携帯用消費者装置は、ウォーターマークに埋め込まれたコンテンツの使用条件を処理するために、エンドユーザ・プレーヤ・アプリケーション195の諸機能のサブセットを実行することができる。エンドユーザおよびエンドユーザ・プレーヤ・アプリケーション195という用語は、これを通して、その使用またはエンドユーザ装置109上での実行を通して意味するために使用する。

【0045】6. 伝送インフラストラクチャ107

セキュア・デジタル・コンテンツ電子配布システム100は、電子デジタル・コンテンツ・ストア103とエンドユーザ装置109とを接続する伝送ネットワークとは無関係のものである。これは、インターネットなどのポイントツーポイント配布モデルと、デジタル同報

通信テレビなどの同報通信配布モデルの両方をサポートする。

【0046】同じツールおよびアプリケーションを使用して様々な伝送インフラストラクチャ107によりコンテンツ113のトランザクションを取得し、パッケージ化し、追跡する場合でも、顧客にサービスを送達する際のプレゼンテーションおよび方法は、選択したインフラストラクチャおよび配布モデルに応じて様々になる可能性がある。また、低帯域インフラストラクチャより高帯域インフラストラクチャの方がより容認できる応答時間で高品質のデジタル・コンテンツを送達できるので、転送中のコンテンツ113の品質も様々になる可能性がある。ポイントツーポイント配布モデル用に設計されたサービス・アプリケーションは、同報通信配布モデルもサポートするように適合させることができる。

【0047】C. システム用途

セキュア・デジタル・コンテンツ電子配布システム100により、諸費者またはビジネスのいずれであっても、エンドユーザ装置109にコンテンツ113の高品質な電子コピーを確実に送達することができ、コンテンツ113の使用を規制し追跡することができる。

【0048】セキュア・デジタル・コンテンツ電子配布システム100は、新しい流通経路と既存の流通経路をともに使用して、様々な消費者サービスおよびビジネス間サービスに配備することができるだろう。特定の各サービスは、セキュア・デジタル・コンテンツ電子配布システム100の権利管理機能により実施可能な異なる金融モデルを使用することができるだろう。卸売りまたは小売り用の購入、ペイパバリッスン使用、加入サービス、コピー／コピー禁止制限、または再配布などのモデルは、クリアリング・ハウス105の権利管理とエンドユーザ・プレーヤ・アプリケーション195のコピー保護機能により実現することができるだろう。

【0049】セキュア・デジタル・コンテンツ電子配布システム100により、電子デジタル・コンテンツ・ストア103および中間市場パートナーには、コンテンツ113を販売するサービスを作成する際に多大な柔軟性が与えられる。同時に、このシステムは、コンテンツ・プロバイダ101に対し、コンテンツ113のライセンスに対する適切な補償が受けられるようにそのデジタル資産が保護され計量されるという一定のレベルの保証を提供する。

【0050】II. 暗号概念およびセキュア・デジタル・コンテンツ電子配布システムへの応用

セキュア・デジタル・コンテンツ電子配布システム100内のライセンス制御は暗号の使用に基づくものである。この項では、本発明の基本的な暗号技術を紹介する。公開キー暗号化、対称キー暗号化、デジタル・シ

グニチャ、デジタル・ウォーターマーク、デジタル証書の使用が知られている。

【0051】A. 対称アルゴリズム

セキュア・デジタル・コンテンツ電子配布システム100では、コンテンツ・プロバイダ101は、対称アルゴリズムを使用してコンテンツを暗号化する。同じキーを使用してデータを暗号化し、暗号化解除するので、このアルゴリズムは対称アルゴリズムと呼ばれる。データ送信側とメッセージ受信側はこのキーを共用しなければならない。共用キーはここでは対称キーという。セキュア・デジタル・コンテンツ電子配布システム100のアーキテクチャは、特定の実施用に選択した特定の対象アルゴリズムとは無関係のものである。

【0052】一般的な対称アルゴリズムは、DES、RC2、RC4である。DESとRC2はどちらもブロック暗号である。ブロック暗号は、一度に1ブロック分のデータ・ビットを使用してデータを暗号化する。DESは、公式の米国政府暗号化規格であり、64ビットのブロック・サイズを有し、56ビットのキーを使用する。トリプルDESは、単純なDESによって達成されるセキュリティを増加するために一般に使用されている。RC2は、RSAデータ・セキュリティによって設計されたものである。RC2は、可変キーサイズ暗号を使用し、64ビットのブロック・サイズを有する。同じくRSAデータ・セキュリティによって設計されたRC4は、可変キーサイズ・ストリーム暗号である。ストリーム暗号は、一度に単一データ・ビットを操作する。RSAデータ・セキュリティでは、RC4の場合、出力バイトあたり8～16回のマシン操作が必要であると主張している。

【0053】IBMでは、SEALという高速アルゴリズムを設計した。SEALは、可変長キーを使用し、32ビット・プロセッサ用に最適化されたストリーム・アルゴリズムである。SEALでは、データ・バイトあたり約5つの基本的なマシン命令を必要とする。使用した160ビット・キーがすでに前処理されて内部テーブルに入っている場合、50MHzで486ベースのコンピュータは7.2メガバイト／秒でSEALコードを実行する。

【0054】マイクロソフトでは、同社のCryptoAPIの概要に関する文書で暗号化性能ベンチマークの結果を報告している。この結果は、Windows NT 4.0を搭載した120MHzのペンティアムベースのコンピュータ上でマイクロソフトのCryptoAPIを使用するアプリケーションを実行することによって得られたものである。

【0055】

【表1】

暗号	キー・サイズ	キー・セットアップ時間	暗号化速度
DES	56	460	1,138,519
RC2	40	40	286,888
RC4	40	151	2,377,723

【0056】B. 公開キー・アルゴリズム

セキュア・デジタル・コンテンツ電子配布システム100では、公開キーを使用して対称キーおよびその他の小さいデータ・ピースを暗号化する。公開キー・アルゴリズムでは、2つのキーを使用する。この2つのキーは、一方のキーで暗号化したデータがもう一方のキーのみによって暗号化解除できるように数学的に関連付けられている。これらのキーのオーナーは、一方のキーを秘密（秘密キー）に保ち、第2のキー（公開キー）を公に配布する。

【0057】公開キー・アルゴリズムを使用した機密メッセージの伝送を確保するために、受信側の公開キーを使用してメッセージを暗号化しなければならない。関連の秘密キーを有する受信側だけがそのメッセージを暗号化解除することができる。また、公開キー・アルゴリズムは、デジタル・シグニチャを生成するためにも使用する。秘密キーはその目的に使用する。以下の項ではデジタル・シグニチャに関する情報を示す。

【0058】最も一般的に使用する公開キー・アルゴリズムは、RSA公開キー暗号である。これは、業界では事実上の公開キー標準になっている。同じく暗号化およびデジタル・シグニチャのために十分機能する他のアルゴリズムとしては、ElGamalとRabinがある。RSAは可変キー長暗号である。

【0059】対称キー・アルゴリズムは公開キー・アルゴリズムよりかなり高速である。ソフトウェアでは、一般にDESはRSAの少なくとも100倍の速度である。このため、RSAはバルク・データの暗号化に使用しない。RSAデータ・セキュリティは、90MHzのペンティアム・マシンではRSAデータ・セキュリティのツールキットBSAFE3.0の秘密キー動作（秘密キーを使用する暗号化または暗号化解除）のスループットが512ビット・モジュールでは21.6キロビット／秒になり、1024ビット・モジュールでは7.4キロビット／秒になると報告している。

【0060】C. デジタル・シグニチャ

セキュア・デジタル・コンテンツ電子配布システム100では、SCの発行者は、デジタル方式でそれにサインすることによりSCの完全性を保護する。一般に、あるメッセージのデジタル・シグニチャを作成するために、メッセージ・オーナーはまずメッセージ・ダイジェスト（以下に定義する）を計算し、次にオーナーの秘密キーを使用してそのメッセージ・ダイジェストを暗号化する。メッセージはそのシグニチャとともに配布される。

メッセージの受信側は、まずメッセージ・オーナーの公開キーを使用してシグニチャを暗号化解除してメッセージ・ダイジェストを回復することにより、デジタル・シグニチャを検証することができる。次に、受信側は、受信したメッセージのダイジェストを計算し、そのダイジェストと回復したダイジェストとを比較する。配布中にメッセージが変更されていない場合、計算したダイジェストと回復したダイジェストは等しくなければならない。

【0061】セキュア・デジタル・コンテンツ電子配布システム100では、SCは複数のデータ・パーツを含むので、各パーツごとにダイジェストが計算され、連結したパーツ・ダイジェストについて要約ダイジェストが計算される。要約ダイジェストは、SCの発行者の秘密キーを使用して暗号化される。暗号化要約ダイジェストは、SC用の発行者のデジタル・シグニチャになる。パーツ・ダイジェストとデジタル・シグニチャはSCの本体に含まれる。SCの受信側は、受信したデジタル・シグニチャとパーツ・ダイジェストにより、SCとそのパーツの完全性を検証することができる。

【0062】メッセージ・ダイジェストを計算するために一方ハッシュ・アルゴリズムを使用する。ハッシュ・アルゴリズムは、可変長入力メッセージを取得し、それを固定長ストリングであるメッセージ・ダイジェストに変換する。一方ハッシュ・アルゴリズムは、1つの方向でのみ動作する。すなわち、入力メッセージ用のダイジェストを計算することは容易であるが、そのダイジェストから入力メッセージを生成することは非常に困難（計算上、実行不可能）である。一方ハッシュ関数の特性により、メッセージ・ダイジェストをそのメッセージのフィンガプリントと見なすことができる。

【0063】より一般的な一方ハッシュ関数は、RSAデータ・セキュリティによるMD5と、米国National Institute of Technology and Standards (NITS) によって設計されたSHAである。

【0064】D. デジタル証書

デジタル証書は、デジタル方式でサインしたメッセージを送信した人物またはエンティティのアイデンティティを立証または検証するために使用する。証書は、公開キーのある人物またはエンティティにバインドする、証明機関によって発行されたデジタル文書である。この証書は、公開キー、人物またはエンティティの名前、満了日、証明機関の名称、その他の情報を含む。また、証書は、証明機関のデジタル・シグニチャも含む。

【0065】あるエンティティ（または人物）がその公開キーでサインし、そのデジタル証書を添付したメッセージを送信すると、そのメッセージの受信側は証書からそのエンティティの名前を使用して、そのメッセージを受け入れるかどうかを判断する。

【0066】セキュア・デジタル・コンテンツ電子配布システム100では、エンドユーザ装置109が発行したものを除くすべてのSCは、そのSCの作成者の証書を含む。エンドユーザ装置109はそのSC内に証書を含む必要はない。というのは、多くのエンドユーザは非真正証明機関によって発行された証書を取得するかまたは証書を有する必要がないからである。セキュア・デジタル・コンテンツ電子配布システム100のクリアリング・ハウス105は、電子デジタル・コンテンツ・ストア103に証書を発行する選択権を有する。このため、エンドユーザ装置109は、電子デジタル・コンテンツ・ストア103がセキュア・デジタル・コンテンツ電子配布システム100によって許可されていることを独立して検証することができる。

【0067】E. SC図形表現のガイド

本書では、SCを図形表現するために、暗号化パーツ、非暗号化パーツ、暗号化キー、証書を示す図面を使用する。次に図5を参照すると、同図はSC200の図面例である。SCの図では以下の記号を使用する。キー201は公開キーまたは秘密キーである。キーの歯はキー・オーナーを示し、たとえば、クリアリングハウスの場合は*

*CLRNGHである。ハンドル内部のPBはそれが公開キーであることを示し、したがって、キー201はクリアリングハウスの公開キーである。ハンドル内部のPVはそれが秘密キーであることを示す。菱形はエンドユーザ・デジタル・シグニチャ202である。頭文字はどの秘密キーを使用してそのシグニチャを作成したかを示し、したがって、EUは以下の表によればエンドユーザのデジタル・シグニチャである。対称キー203はコンテンツを暗号化するために使用する。暗号化対称キー・オブジェクト204は、CLRNGHのPBで暗号化した対称キー203を含む。その長方形の上縁にあるキーはそのオブジェクトの暗号化で使用するキーである。長方形内部の記号またはテキストは、暗号化オブジェクト（この場合は対称キー）を示す。この例ではトランザクションID暗号化オブジェクト205である、もう一つの暗号化オブジェクトを示す。また、コンテンツ・ライセンス管理用の使用条件206は以下に記載する通りである。SC200は、使用条件206と、トランザクションID暗号化オブジェクト205と、アプリケーションID暗号化オブジェクト207と、暗号化対称キー・オブジェクト204とを含み、いずれもエンドユーザ・デジタル・シグニチャ202でサインされている。

【0068】以下の表は、SCの署名者を識別する頭文字を示している。

【0069】

【表2】

頭文字	コンポーネント
CP	コンテンツ・プロバイダ101
MS	電子デジタル・コンテンツ・ストア103
HS	コンテンツ・ホスト・サイト111
EU	エンドユーザ装置109
CH	クリアリング・ハウス105
CA	証明機関（図示せず）

【0070】F. セキュア・コンテナ暗号化の例

以下の表および図は、SCからの情報を作成し回復するために使用する暗号化および暗号化解除プロセスの概要を示す。このプロセス概要で作成され暗号化解除されるSCは一般的なSCである。これは、セキュア・デジタル・コンテンツ電子配布システム100における権利管理に使用する特定のSCタイプのいずれかを表すものではない。このプロセスは、暗号化プロセスについて図6に記載した諸ステップからなるものである。

【0071】図6の暗号化プロセスのプロセス・フローステップ プロセス

301 送信側はランダムな対称キーを生成し、それを使用してコンテンツを暗号化する。

302 送信側はハッシュ・アルゴリズムにより暗号化コンテンツを実行して、コンテンツ・ダイジェストを

生成する。

303 送信側は受信側の公開キーを使用して対称キーを暗号化する。PBRECPNTは受信側の公開キーを意味する。

304 送信側はステップ302で使したのと同じハッシュ・アルゴリズムにより暗号化対称キーを実行して、対称キー・ダイジェストを生成する。

305 送信側はステップ302で使したのと同じハッシュ・アルゴリズムによりコンテンツ・ダイジェストと対称キー・ダイジェストの連結を実行して、SCダイジェストを生成する。

306 送信側は送信側の秘密キーでSCダイジェストを暗号化して、SC用のデジタル・シグニチャを生成する。PVSENDERは送信側の秘密キーを意味する。

307B 送信側は、暗号化コンテンツ、暗号化対称キー、コンテンツ・ダイジェスト、対称キー・ダイジェスト、送信側の証書、SCシグニチャを含むSCファイルを作成する。

307A 送信側は安全な通信を開始する前に証明機関から証書入手していただなければならない。証明機関は、送信側の公開キーと、送信側の名前をその証書に含め、それにサインする。PV CAUTHRは証明機関の秘密キーを意味する。送信側は受信側にSCを伝送する。

【0072】図7の暗号化解除プロセスのプロセス・フロー

ステップ プロセス

408 受信側はSCを受信し、そのパーツを分解する。

409 受信側は、証明機関の公開キーでそれを暗号化解除することにより、送信側の証書内のデジタル・シグニチャを検証する。証書のデジタル・シグニチャが有効である場合、受信側は証書から送信側の公開キーを取得する。

410 受信側は送信側の公開キーを使用してSCのデジタル・シグニチャを暗号化解除する。これでSCダイジェストを回復する。PB SENDERは送信側の公開キーを意味する。

411 受信側は送信側が使用したのと同じハッシュ・アルゴリズムにより受信コンテンツ・ダイジェストと暗号化キー・ダイジェストの連結を実行して、SCダイジェストを計算する。

412 受信側は、計算したSCダイジェストと送信側のデジタル・シグニチャにより回復したダイジェストとを比較する。両者が同じである場合、受信側は、受信ダイジェストが変更されていないことを確認し、暗号化解除プロセスを続行する。両者が同じではない場合、受信側はそのSCを破棄し、送信側に通知する。

413 受信側はステップ411で使用したのと同じハッシュ・アルゴリズムにより暗号化対称キーを実行して、対称キー・ダイジェストを計算する。

414 受信側は、計算した対称キー・ダイジェストとSCで受信したダイジェストとを比較する。これが同じである場合、受信側は、暗号化対称キーが変更されていないことを把握する。受信側は暗号化解除プロセスを続行する。これが有効ではない場合、受信側はそのSCを破棄し、送信側に通知する。

415 受信側はステップ411で使用したのと同じハッシュ・アルゴリズムにより暗号化コンテンツを実行して、コンテンツ・ダイジェストを計算する。

416 受信側は、計算したコンテンツ・ダイジェストとSCで受信したダイジェストとを比較する。これが同じである場合、受信側は、暗号化コンテンツが変更されていないことを把握する。次に受信側は暗号化解除プロセスを続行する。これが有効ではない場合、受信側は

そのSCを破棄し、送信側に通知する。

417 受信側は、受信側の秘密キーを使用して暗号化対称キーを暗号化解除する。これで対称キーを回復する。PV RECPNTは受信側の秘密キーを意味する。

418 受信側は対称キーを使用した暗号化コンテンツを暗号化解除する。これでコンテンツを回復する。

【0073】III. セキュア・デジタル・コンテンツ電子配布システムのフロー

セキュア・デジタル・コンテンツ電子配布システム100は、システムの様々な関係者が使用する複数のコンポーネントからなるものである。このような関係者としては、コンテンツ・プロバイダ101、電子デジタル・コンテンツ・ストア103、エンドユーザ装置109によるエンドユーザ、クリアリング・ハウス105を含む。セキュア・デジタル・コンテンツ電子配布システム100の概要として高レベル・システム・フローを使用する。以下に概略を示すこのフローは、システム100全体を通過するコンテンツを追跡する。そのうえ、このフローは、コンテンツ113の購入、ロック解除、使用のためのトランザクションを実行するために関係者が使用する諸ステップの概略を示す。このシステム・フローで行う想定の一部としては以下のものを含む。

- ・ これは、デジタル・コンテンツ・サービス（PCへのポイントツーポイント・インタフェース）用のシステム・フローである。

- ・ コンテンツ・プロバイダ101は、（音楽オーディオ例として）PCM未圧縮フォーマットでオーディオ・デジタル・コンテンツを提示する。

- ・ コンテンツ・プロバイダ101はODBC適合データベース内にメタデータを有するか、あるいはコンテンツ・プロバイダ101はコンテンツ情報処理サブシステム内にデータを直接入力するかまたは規定のASCIIファイル・フォーマットでデータをすでに提供していることになる。

- ・ 金融上の決済は電子デジタル・コンテンツ・ストアによって行われる。

- ・ コンテンツ113は単一コンテンツ・ホスト・サイト111でホストとして処理される。

【0074】当業者であれば、これらの想定は、同報通信されるデジタル・コンテンツ、たとえば、音楽、ビデオ、プログラムならびに電子配布システムの正確な性質に対処するように変更することができることに留意されたい。

【0075】以下のプロセス・フローは図1ないし図4に示されている。

ステップ プロセス

121 未圧縮PCMオーディオ・ファイルはコンテンツ・プロバイダ101によってコンテンツ113として提供される。そのファイル名は、コンテンツ113用

のコンテンツ・プロバイダ101の固有の識別子とともにワーク・フロー・マネージャ154ツール内に入力される。

122 メタデータは、コンテンツ113用のコンテンツ・プロバイダ101の固有の識別子とデータベース・マッピング・テンプレートによって提供される情報を使用して、コンテンツ情報処理サブシステムによってコンテンツ・プロバイダのデータベース160から取り込まれる。

123 ワーク・フロー・マネージャ・ツール154 10 は、コンテンツ・プロバイダ101での収集作成プロセスによりコンテンツ・フローを指示するために使用する。また、これは、任意の時点でシステム内のコンテンツ・ピースの状況を追跡するために使用することもできる。

124 コンテンツ113用の使用条件はコンテンツ情報処理サブシステム内に入力されるが、これは手動または自動のいずれでも行うことができる。このデータは、コピー制限規則と、必要と見なされたその他のビジネス規則を含む。メタデータの入力はすべて、そのデータのオーディオ処理と並行して行うことができる。

125 ウォータマーク・ツールは、コンテンツを識別するためにコンテンツ・プロバイダ101が必要と見なすデータをコンテンツ113内に隠すために使用する。これは、それがいつ取り込まれたか、それがどこから来たか（この場合はコンテンツ・プロバイダ101）と、コンテンツ・プロバイダ101によって指定されたその他の情報を含むことができるだろう。

・ コンテンツ処理ツール125は、サポートされる様々な圧縮レベルの必要に応じて、コンテンツ113への等化、強弱の変化の調節、再サンプリングを実行する。

・ コンテンツ113は、コンテンツ処理ツール125を使用して所望の圧縮レベルまで圧縮される。次にコンテンツ113を再生して、この圧縮によって必要なレベルのコンテンツ113品質が得られることを検証することができる。必要であれば、等化、強弱の変化の調節、圧縮、再生品質チェックを所望な回数だけ実行することができる。

・ コンテンツ113とそのメタデータのサブセット 40 は、SCバックカによって対称キーで暗号化される。次にこのツールは、クリアリング・ハウス105の公開キーを使用してそのキーを暗号化し、暗号化対称キーを生成する。それを暗号化解除できるエンティティはクリアリング・ハウス105だけなので、このキーはコンテンツ113のセキュリティを損なわずにどこにでも伝送することができる。

126 次に、暗号化対称キー、メタデータ、コンテンツ113に関するその他の情報はSCバックカ・ツール152によってメタデータSC内にバックされる。

127 次に、暗号化コンテンツ113とメタデータ 50

はコンテンツSC内にバックされる。この時点で、コンテンツ113とメタデータに関する処理は完了する。

128 次に、メタデータSCは、コンテンツ分配ツール（図示せず）を使用してコンテンツ・プロモーション・ウェブ・サイト156に送られる。

129 コンテンツ分配ツールはコンテンツSCをコンテンツ・ホスト・サイト111に送る。コンテンツ・ホスト・サイトは、コンテンツ・プロバイダ101、クリアリング・ハウス105、またはコンテンツ・ホスト専用の特別な位置に存在することができる。このサイト用のURLは、メタデータSCに追加されたメタデータの一部である。

130 コンテンツ・プロモーション・ウェブ・サイト156は、システム100に追加された新しいコンテンツ113を電子デジタル・コンテンツ・ストア103に通知する。

131 コンテンツ収集ツールを使用して、電子デジタル・コンテンツ・ストア103は次に、それらが販売したいと希望するコンテンツ113に対応するメタデータSCをダウンロードする。

132 電子デジタル・コンテンツ・ストア103は、コンテンツ収集ツールを使用して、自分のウェブ・サイト上でコンテンツ113をプロモートするために使用したいと希望する任意のデータをメタデータSCから引き出すことになる。このメタデータの各部分へのアクセスは、所望であれば保護し支払い請求することができる。

133 この電子デジタル・コンテンツ・ストア103に固有のコンテンツ113用の使用条件は、コンテンツ収集ツールを使用して入力される。このような使用条件としては、コンテンツ113の様々な圧縮レベルに応じた小売価格、コピー／再生制限を含む。

134 電子デジタル・コンテンツ・ストア103固有の使用条件および元のメタデータSCは、SCバックカ・ツールによってオフターSC内にバックされる。

135 電子デジタル・コンテンツ・ストア103のウェブ・サイトを更新した後、コンテンツ113はウェブをサーフィンしているエンドユーザに使用可能なものになる。

136 エンドユーザが購入したいと希望するコンテンツ113を見つけると、エンドユーザは音楽アイコンなどのコンテンツ・アイコンをクリックし、その項目は、電子デジタル・コンテンツ・ストア103によって維持されているそのエンドユーザのショッピング・カートに追加される。エンドユーザはショッピングを完了すると、処理のために電子デジタル・コンテンツ・ストア103に購入要求を提示する。

137 次に電子デジタル・コンテンツ・ストア103は、クレジット・カード清算組織と対話して、現在ビジネスを行っているのと同じように資金を確保する。

138 電子デジタル・コンテンツ・ストア103はクレジット・カード清算組織からクレジット・カード認証番号を受け取ると、これをデータベース内に記憶し、SCバック・ツールを呼び出してトランザクションSCを構築する。このトランザクションSCは、エンドユーザが購入したコンテンツ113用のオファーSCのすべてと、電子デジタル・コンテンツ・ストア103まで追跡可能なトランザクションIDと、エンドユーザを識別する情報と、圧縮レベルと、使用条件と、購入した歌曲の価格リストを含む。

139 次にこのトランザクションSCはエンドユーザ装置109に伝送される。

140 トランザクションSCは、エンドユーザ装置109に到着すると、トランザクションSCをオープンし、エンドユーザの購入を承認するエンドユーザ・プレーヤ・アプリケーション195を開始する。次にエンドユーザ・プレーヤ・アプリケーション195は個々のオファーSCをオープンし、代替実施形態ではダウンロード時間の推定値をユーザに通知することができる。次にそのアプリケーションは、いつコンテンツ113をダウンロードしたいのかを指定するようユーザに要求する。

141 エンドユーザがダウンロードを要求した時間に基づいて、エンドユーザ・プレーヤ・アプリケーション195はウェイクアップし、とりわけコンテンツ113用の暗号化対称キーと、トランザクションIDと、エンドユーザ情報とを含むオーダSCを構築することにより、ダウンロード・プロセスの始動を開始することになる。

142 次にこのオーダSCは処理のためにクリアリング・ハウス105に送られる。

143 クリアリング・ハウス105はオーダSCを受け取り、それをオープンし、いずれのデータも改竄されていないことを検証する。クリアリング・ハウス105は、エンドユーザによって購入された使用条件を妥当性検査する。このような使用条件は、コンテンツ・プロバイダ101によって指定されたものと適合しなければならない。この情報はデータベースにログインされる。

144 すべてのチェックが完了すると、暗号化対称キーはクリアリング・ハウス105の秘密キーを使用して暗号化解除される。次に対称キーは、エンドユーザの公開キーを使用して暗号化される。この新しい暗号化対称キーは次にSCバックによってライセンスSC内にパッケージ化される。

145 次にライセンスSCはエンドユーザに伝送される。

146 ライセンスSCはエンドユーザ装置109側で受信されると、コンテンツSCがダウンロードされるまでメモリ内に記憶される。

147 エンドユーザ装置109は、購入したコンテンツ113用の対応ライセンスSCを送信して、コンテ

ンツ・ホスト設備111から要求する。

148 コンテンツ113はエンドユーザ装置109に送られる。受信次第、コンテンツ113は対称キーを使用してエンドユーザ装置109によって暗号化解除される。

【0076】IV. 権利管理アーキテクチャ・モデル

A. アーキテクチャ層機能

図8は、セキュア・デジタル・コンテンツ電子配布システム100の権利管理アーキテクチャのブロック図である。アーキテクチャ上、ライセンス制御層501、コンテンツ識別層503、コンテンツ使用制御層505、コンテンツ・フォーマット層507という4つの層がセキュア・デジタル・コンテンツ電子配布システム100を表している。各層の全体的な機能目標と、各層の個々の重要機能について、この項で説明する。各層の機能は他の層の機能とはまったく無関係である。広範囲の制限内で各層の機能は、他の層の機能性に影響せずと同様の機能で代用することができる。明らかに、ある層からの出力は隣接層にとって容認できるフォーマットおよびセマンティクスを満足する必要がある。

【0077】ライセンス制御層501は以下の点を保証するものである。

- ・ デジタル・コンテンツは配布中に違法インターセプトおよび改竄から保護される。

- ・ コンテンツ113は正当なコンテンツ・オーナーから発生し、ライセンス配布者、たとえば、電子デジタル・コンテンツ・ストア103によって配布される。

- ・ デジタル・コンテンツ購入者は適切にライセンスを受けたアプリケーションを有する。

- ・ 配布者は、コンテンツ113のコピーが購入者またはエンドユーザに使用可能なものになる前に、購入者から支払を受ける。

- ・ 報告のためにトランザクションの記録が保持される。

【0078】コンテンツ識別層503は、著作権およびコンテンツ購入者のアイデンティティの検証を可能にするものである。コンテンツの著作権情報およびコンテンツ購入者のアイデンティティにより、認可されているか否かにかかわらず、コンテンツ113のすべてのコピーのソース追跡が可能になる。したがって、コンテンツ識別層503は著作権侵害と闘うための手段を提供する。

【0079】コンテンツ使用制御層505は、コンテンツ113のコピーがストア使用条件519に応じて購入者の装置内で使用されることを保証するものである。ストア使用条件519は、コンテンツ113について許される再生回数およびローカル・コピー数と、コンテンツ113を外部携帯用装置に記録可能であるかどうかを指定することができる。コンテンツ使用制御層505内の諸機能は、コンテンツのコピー／再生使用を追跡し、コピー／再生状況を更新する。

【0080】コンテンツ・フォーマット層507は、コンテンツ・オーナーの設備内でのその固有表現からセキュア・デジタル・コンテンツ電子配布システム100のサービス機能および配布手段に適合する形式へのコンテンツ113のフォーマット変換を可能にするものである。この変換処理は、圧縮コード化と、周波数等化および振幅ダイナミック調整など、それに関連する前処理とを含むことができる。コンテンツ113がオーディオである場合、購入者側では、再生または携帯用装置への転送に適したフォーマットを達成するように受信したコンテンツ113を処理する必要もある。

【0081】B. 機能区分およびフロー

権利管理アーキテクチャ・モデルを図8に示すが、これはセキュア・デジタル・コンテンツ電子配布システム100を構成する動作コンポーネントに対するアーキテクチャ層のマッピングと、各層の重要機能を示している。

【0082】1. コンテンツ・フォーマット層507
コンテンツ・フォーマット層507に関連する一般的な機能は、コンテンツ・プロバイダ101でのコンテンツ前処理502および圧縮511と、エンドユーザ装置109でのコンテンツ・スクランブル解除513および圧縮解除515である。前処理の必要性和特定の機能の例については前述した通りである。コンテンツ圧縮511は、コンテンツ113のファイル・サイズとその伝送時間を低減するために使用する。セキュア・デジタル・コンテンツ電子配布システム100では、コンテンツ113および伝送媒体のタイプに適した任意の圧縮アルゴリズムを使用することができる。音楽の場合、MPEG 1/2/4、ドルビーAC-2およびAC-3、ソニー適応変換コーディング(ATRAC)、低ビット伝送速度アルゴリズムは、通常使用される圧縮アルゴリズムの一部である。コンテンツ113は、必要な記憶サイズを低減するために圧縮した形式でエンドユーザ装置109に記憶される。これは、アクティブ再生中に圧縮解除される。また、アクティブ再生中にはスクランブル解除も行われる。スクランブルの目的およびタイプについては、コンテンツ使用制御層505の説明時に後述する。

【0083】2. コンテンツ使用制御層505

コンテンツ使用制御層505は、エンドユーザ装置109でのコンテンツ113の使用に課せられる条件または制限の指定および執行を可能にする。この条件は、コンテンツ113について許される再生回数、コンテンツ113の2次コピーが許されるかどうか、2次コピーの数、コンテンツ113を外部携帯用装置にコピー可能かどうかを指定することができる。コンテンツ・プロバイダ101は、許容できる使用条件517を設定し、それをSCに入れて電子デジタル・コンテンツ・ストア103に伝送する(ライセンス制御層501の項を参照)。それによってコンテンツ・プロバイダ101が設

定した元の条件が無効にならない限り、電子デジタル・コンテンツ・ストア103は使用条件517を大きくするかまたは狭くすることができる。次に電子デジタル・コンテンツ・ストア103はすべてのストア使用条件519を(SCに入れて)エンドユーザ装置109およびクリアリング・ハウス105に伝送する。クリアリング・ハウス105は、エンドユーザ装置109へのコンテンツ113のリリースを許可する前に、使用条件妥当性検査521を実行する。

【0084】コンテンツの使用条件517の執行は、エンドユーザ装置109内のコンテンツ使用制御層505によって実行される。第1に、コンテンツ113を受信すると、エンドユーザ装置109内のコンテンツ識別層503からのコピーは、初期コピー/再生許可を表すコピー/再生コード523でコンテンツ113にマークを付ける。第2に、プレーヤ・アプリケーション195は、それをエンドユーザ装置109に記憶する前にコンテンツ113に暗号法でスクランブルをかける。プレーヤ・アプリケーション195は各コンテンツ項目ごとにスクランブル・キーを生成し、そのキーは暗号化され、エンドユーザ装置109に隠される。次に、エンドユーザ109がコピーまたは再生のためにコンテンツ113にアクセスするたびに、エンドユーザ装置109は、コンテンツ113のスクランブル解除と再生またはコピーの実行を許可する前にコピー/再生コードを検証する。また、エンドユーザ装置109は、コンテンツ113のオリジナル・コピー内または新しい2次コピー上のコピー/再生コードを適切に更新する。コピー/再生コーディングは、圧縮されたコンテンツ113について実行される。すなわち、コピー/再生コードを埋め込む前にコンテンツ113を圧縮解除する必要はない。

【0085】エンドユーザ装置109は、ライセンス・ウォータマーク527を使用してコンテンツ113内にコピー/再生コードを埋め込む。埋め込まれたデータを読み取ったり変更することができるのは、埋め込まれたアルゴリズムと関連のスクランブル・キーを良く知っているエンドユーザ・プレーヤ・アプリケーション195のみである。このデータは人間の監視者にとっては目に見えないかまたは聞こえないものであり、すなわち、このデータはコンテンツ113に対して感知できるほどの劣化をもたらすことはない。ウォータマークはコンテンツ処理、データ圧縮、D/A変換およびA/D変換、通常のコンテンツ処理によってもたらされる信号劣化といういくつかのステップ後も存続するので、ウォータマークはアナログ表現を含む任意の表現形式でコンテンツ113とともに持続する。代替実施形態では、ライセンス・ウォータマーク527を使用してコピー/再生コードをコンテンツ113内に埋め込む代わりに、エンドユーザ・プレーヤ・アプリケーション195は確実に記憶した使用条件519を使用する。

【0086】3. コンテンツ識別層503

コンテンツ識別層503の一部として、コンテンツ・プロバイダ101は、ライセンス・ウォーターマーク527を使用して、コンテンツ識別子、コンテンツ・オーナーなどのデータと、出版日、配布地域などのその他の情報をコンテンツ113に埋め込む。このウォーターマークはここでは著作権ウォーターマーク529という。受領すると、エンドユーザ装置109はコンテンツ113のコピーにコンテンツ購入者の名前とトランザクションID535（以下のライセンス制御層501の項を参照）、ならびにライセンス日や使用条件517などのその他の情報でウォーターマークを付ける。このウォーターマークはここではライセンス・ウォーターマークという。承認された方法で入手したまたはそうではなく、コンテンツ品質を保存するオーディオ処理の対象となるコンテンツ113のいずれのコピーにも、著作権ウォーターマークとライセンス・ウォーターマークが付いている。コンテンツ識別層503は著作権侵害を阻止するものである。

【0087】4. ライセンス制御層501

ライセンス制御層501は、無許可インターセプトからコンテンツ113を保護し、エンドユーザ装置109に適切にライセンスを与え、認可電子デジタル・コンテンツ・ストア103とのライセンス購入トランザクションを正常に完了したエンドユーザに対してのみコンテンツが個別にリリースされることを保証する。ライセンス制御層501は二重暗号化531によってコンテンツ113を保護する。コンテンツ113はコンテンツ・プロバイダ101によって生成された暗号化対称キーを使用して暗号化され、その対称キーはクリアリング・ハウスの公開キー621を使用して暗号化される。最初に対称キーを回復できるのはクリアリング・ハウス105のみである。

【0088】ライセンス制御は、「信頼できる当事者」としてクリアリング・ハウス105とともに設計されている。ライセンス要求537（すなわち、エンドユーザ装置109へのコンテンツ113用の対称キー623）に関する許可をリリースする前に、クリアリング・ハウス105は、トランザクション541とライセンス認可543が完全かつ真正であること、電子デジタル・コンテンツ・ストア103が電子コンテンツ113の販売に関してセキュア・デジタル・コンテンツ電子配布システム100からの認可を得ていること、エンドユーザが適切にライセンスを受けたアプリケーションを有することを検証する。監査／報告545により、報告書を作成することができ、セキュア・デジタル・コンテンツ電子配布システム100内の他の認可当事者とライセンス・トランザクション情報を共用することができる。

【0089】ライセンス制御はSC処理533により実施される。SCは、システム動作コンポーネント間で暗号化コンテンツ113と情報を配布するために使用する

（詳細については以下のSCの詳細構造の項を参照）。SCは、暗号化、デジタル・シグニチャ、デジタル証書を使用して電子情報またはコンテンツ113を無許可インターセプトおよび変更から保護する情報の暗号キャリアである。また、これは、電子データの信憑性検証も可能にする。

【0090】ライセンス制御では、コンテンツ・プロバイダ101、電子デジタル・コンテンツ・ストア103、クリアリング・ハウス105が、このようなコンポーネントを立証するために使用する、評判の良い証明機関からの真正の暗号デジタル証書を有することが必要である。エンドユーザ装置109はデジタル証書を有する必要はない。

【0091】C. コンテンツ配布ライセンス制御

図9は、図8のライセンス制御層に適用されたときのコンテンツ配布ライセンス制御の概要を示すブロック図である。同図では、電子デジタル・コンテンツ・ストア103と、エンドユーザ装置109と、クリアリング・ハウス105がインターネットを介して相互接続され、これらのコンポーネント間でユニキャスト（ポイントツーポイント）伝送を使用することを示している。コンテンツ・プロバイダ101と電子デジタル・コンテンツ・ストア103との通信も、インターネットまたはその他のネットワークによる可能性がある。エンドユーザ装置109と電子デジタル・コンテンツ・ストア103とのコンテンツ購入商用トランザクションが標準のインターネット・ウェブ・プロトコルに基づくものであると想定する。ウェブベースの対話の一部として、エンドユーザは、購入するコンテンツ113を選択し、個人情報および金融情報を提供し、購入条件に同意する。電子デジタル・コンテンツ・ストア103は、SETなどのプロトコルを使用して取得機関から支払許可を得ることができる。

【0092】また、図9では、電子デジタル・コンテンツ・ストア103がすでに標準のウェブ・プロトコルに基づいてエンドユーザ・プレーヤ・アプリケーション195をエンドユーザ装置109にダウンロードしたと想定する。このアーキテクチャでは、電子デジタル・コンテンツ・ストア103はダウンロードしたプレーヤ・アプリケーション195に固有のアプリケーションIDを割り当て、後でアプリケーション・ライセンス検証を行うためにエンドユーザ装置109がそれを記憶しなければならない（以下参照）。

【0093】全体的なライセンスの流れはコンテンツ・プロバイダ101から始まる。コンテンツ・プロバイダ101は、ローカルで生成した暗号化対称キーを使用してコンテンツ113を暗号化し、クリアリング・ハウス105の公開キー621を使用して対称キー623を暗号化する。代替実施形態の対称キーは、ローカルで生成する代わりに、クリアリング・ハウス105からコンテ

ンツ・プロバイダ101に送ることもできる。コンテンツ・プロバイダ101は、暗号化コンテンツ113の周りにコンテンツSC630を作成し、暗号化対称キー623、ストア使用条件519、その他のコンテンツ113関連情報の周りにメタデータSC620を作成する。すべてのコンテンツ113オブジェクトについて、1つのメタデータSC620と1つのコンテンツSC630が存在する。コンテンツ113オブジェクトは同一歌曲の圧縮レベルである場合もあれば、コンテンツ113オブジェクトはアルバム上の各歌曲である場合もあり、あるいはコンテンツ113オブジェクトはアルバム全体である場合もある。各コンテンツ113オブジェクトごとに、メタデータSC620は、コンテンツ使用制御層505に関連するストア使用条件519も伝達する。

【0094】コンテンツ・プロバイダ101は、1つまたは複数の電子デジタル・コンテンツ・ストア103にメタデータSC620を配布し（ステップ601）、1つまたは複数のコンテンツ・ホスト・サイトにコンテンツSC630を配布する（ステップ602）。次に各電子デジタル・コンテンツ・ストア103はオファーSC641を作成する。オファーSC641は通常、メタデータSC620と同じ情報の多くを伝達し、コンテンツ・プロバイダ101のデジタル・シグニチャ624およびコンテンツ・プロバイダ101の証書（図示せず）を含む。前述のように、電子デジタル・コンテンツ・ストア103は、初めにコンテンツ・プロバイダ101によって定義されたストア使用条件519（コンテンツ使用制御層が処理する）を大きくするかまたは狭くすることができる。任意選択で、コンテンツSC630またはメタデータSC620あるいはその両方には、コンテンツ・プロバイダ101のデジタル・シグニチャ624でサインする。

【0095】エンドユーザ装置109と電子デジタル・コンテンツ・ストア103とのコンテンツ購入トランザクション（ステップ603）の完了後、電子デジタル・コンテンツ・ストア103はトランザクションSC640を作成し、それをエンドユーザ装置109に転送する（ステップ604）。トランザクションSC640は、固有のトランザクションID535と、購入者の名前（すなわち、エンドユーザの名前）（図示せず）と、エンドユーザ装置109の公開キー661と、購入したコンテンツ113に関連するオファーSC641とを含む。図9のトランザクション・データ642はトランザクションID535とエンドユーザの名前（図示せず）の両方を表している。トランザクション・データ642は、クリアリング・ハウス105の公開キー621で暗号化される。任意選択で、トランザクションSC640には、電子デジタル・コンテンツ・ストア103のデジタル・シグニチャ643でサインする。

【0096】トランザクションSC640（およびそれ

に含まれるオファーSC641）を受け取ると、エンドユーザ装置109上で実行されるエンドユーザ・プレーヤ・アプリケーション195はオファーSC650によりクリアリング・ハウス105からライセンス認可を送信請求する。オファーSC650は、オファーSC641からの暗号化対称キー623およびストア使用条件519と、トランザクションSC640からの暗号化トランザクション・データ642と、エンドユーザ装置109からの暗号化アプリケーションID551とを含む。代替実施形態のオファーSC650には、エンドユーザ装置109のデジタル・シグニチャ652でサインする。

【0097】エンドユーザ装置109からオファーSC650を受け取ると、クリアリング・ハウス105は以下の点を検証する。

1. 電子デジタル・コンテンツ・ストア103がセキュア・デジタル・コンテンツ電子配布システム100から認可を得ている（クリアリング・ハウス105のデータベース160内に存在する）こと。
2. オファーSC650が変更されていないこと。
3. トランザクション・データ642と対称キー623が完全かつ真正であること。
4. エンドユーザ装置109が購入した電子ストア使用条件519がコンテンツ・プロバイダ101が設定した使用条件517に適合していること。
5. アプリケーションID551が有効な構造を有し、それが認可電子デジタル・コンテンツ・ストア103によって提供されたこと。

【0098】この検証が成功した場合、クリアリング・ハウス105は、対称キー623とトランザクション・データ642を暗号化解除し、ライセンスSC660を構築してエンドユーザ装置109に転送する（ステップ606）。ライセンスSC660は対称キー623とトランザクション・データ642を伝達するが、いずれもエンドユーザ装置109の公開キー661を使用して暗号化されている。いずれかの検証が失敗した場合、クリアリング・ハウス105はエンドユーザ装置109へのライセンスを拒否し、エンドユーザ装置109に通知する。また、クリアリング・ハウス105は直ちに電子デジタル・コンテンツ・ストア103にこの検証失敗を通知する。代替実施形態のクリアリング・ハウス105は、そのデジタル・シグニチャ663でライセンスSC660にサインする。

【0099】ライセンスSC660を受け取った後、エンドユーザ装置109は、クリアリング・ハウス105から前に受け取った対称キー623およびトランザクション・データ642を暗号化解除し、コンテンツ・ホスト・サイト111からコンテンツSC630を要求する（ステップ607）。コンテンツSC630が到着すると（ステップ608）、エンドユーザ装置109は、対称キー623を使用してコンテンツ113を暗号化解除

し(ステップ609)、図8に関して前述したようにライセンス・ウォーターマーク、コピー／再生コーディング、スクランブル、その他のコンテンツ113の処理のために、コンテンツ113およびトランザクション・データ642を他の層に渡す。

【0100】最後に、クリアリング・ハウス105は、監査および追跡のために要約トランザクション報告をコンテンツ・プロバイダ101および電子デジタル・コンテンツ・ストア103に定期的に伝送する(ステップ610)。

【0101】V. セキュア・コンテナ構造

A. 一般構造

セキュア・コンテナ(SC)は、相俟ってコンテンツ113のユニットまたはトランザクションの一部分を定義し、また使用条件、メタデータ、暗号化方法などの関連情報も定義する、複数のパーツからなる構造である。SCは、情報の完全性、完璧さ、信憑性を検証できるように設計されている。SC内の情報の一部は、適正な許可を取得した後でなければアクセスできないように暗号化することができる。

【0102】SCは、SCとSCに含まれる各パーツに関する情報のレコードを有する少なくとも1つの素材一覧表(BOM)パーツを含む。各パーツごとに、MD-5などのハッシュ・アルゴリズムを使用してメッセージ・ダイジェストが計算され、そのパーツ用のBOMレコードに含まれる。各パーツのダイジェストはひとまとめに連結され、そのダイジェストからもう1つのダイジェストが計算され、SCを作成するエンティティの秘密キーを使用して暗号化され、デジタル・シグニチャを作成する。SCを受け取る当事者は、そのデジタル・シグニチャを使用してすべてのダイジェストを検証し、SCおよびそのすべてのパーツの完全性および完璧さを妥当性検査することができる。

【0103】以下の情報は、各パーツのレコードとともに、BOM内のレコードとして含めることができる。どのレコードを含める必要があるかは、SCのタイプによって決まる。

- ・ SCのバージョン
- ・ SCのID
- ・ SCのタイプ(たとえば、オファー、オーダー、トランザクション、コンテンツ、メタデータ、プロモーション、ライセンス)
- ・ SCの発行者
- ・ SCが作成された日付
- ・ SCの満了日
- ・ クリアリング・ハウスのURL
- ・ 含まれるパーツに使用するダイジェスト・アルゴリズムの記述(デフォルトはMD-5)
- ・ デジタル・シグニチャ暗号化に使用するアルゴリズムの記述(デフォルトはRSA)

・ デジタル・シグニチャ(含まれるパーツの連結ダイジェストのすべての暗号化ダイジェスト)

【0104】SCは複数のBOMを含むことができる。たとえば、オファーSC641は、そのBOMを含む、元のメタデータSC620の各パーツと、電子デジタル・コンテンツ・ストア103によって追加された追加情報と、新しいBOMからなる。メタデータSC620のBOMのレコードはオファーSC641のBOMに含まれる。このレコードは、その完全性を妥当性検査するために使用可能なメタデータSC620のBOM用のダイジェストを含み、したがって、メタデータSC620に含まれる各パーツの完全性もメタデータSC620のBOMに記憶されたパーツ・ダイジェスト値を使用して妥当性検査することができる。メタデータSC620からのいずれのパーツも、オファーSC641用に作成された新しいBOM内のレコードを有していない。電子デジタル・コンテンツ・ストア103とメタデータSC620のBOMによって追加されたパーツのみが、新しいBOM内のレコードを有する。

【0105】SCはキー記述パーツも含むことができる。キー記述パーツとしては、SC内の暗号化パーツに関する以下の情報を含むレコードを含むことができる。

- ・ 暗号化パーツの名前
- ・ それが暗号化解除されたときにそのパーツのために使用する名前
- ・ そのパーツを暗号化するために使用する暗号化アルゴリズム
- ・ そのパーツを暗号化するために使用した公開暗号化キーを示すためのキー識別子または暗号化解除するときに暗号化パーツを暗号化解除するために使用する暗号化対称キー
- ・ 対称キーを暗号化するために使用する暗号化アルゴリズム。このフィールドはキー記述パーツ内のレコードが暗号化パーツを暗号化するために使用した暗号化対称キーを含む場合のみ存在する。
- ・ 対称キーを暗号化するために使用した公開暗号化キーのキー識別子。このフィールドはキー記述パーツ内のレコードが暗号化対称キーと、暗号化パーツを暗号化するために使用した対称キーの暗号化アルゴリズム識別子を含む場合のみ存在する。SCが暗号化パーツを含まない場合、キー記述パーツは一切存在しない。

【0106】B. 権利管理言語構文およびセマンティクス

権利管理言語は、コンテンツ113の購入後にエンドユーザによるコンテンツ113の使用に関する制限を定義するために値を割り当てることができるパラメータからなる。コンテンツ113の使用に関する制限は使用条件517である。各コンテンツ・プロバイダ101は、そのコンテンツ113の各項目ごとに使用条件517を指定する。電子デジタル・コンテンツ・ストア103

は、メタデータSC620内の使用条件517を解釈し、その情報を使用して、顧客に提示したい選択オプションを提供すると同時にコンテンツ113に関する小売購入情報を追加する。エンドユーザが購入のためにコンテンツ113の項目を選択した後、エンドユーザ装置109はストア使用条件519に基づいてコンテンツ113に関する許可を要求する。クリアリング・ハウス105がエンドユーザにライセンスSC660を送る前に、クリアリング・ハウス105は、要求したストア使用条件519がメタデータSC620内にコンテンツ・プロバイダ101によって指定された許容できる使用条件517と一致していることを検証する。

【0107】エンドユーザ装置109が購入したコンテンツ113を受け取ると、ストア使用条件519はウォーターマーク・ツールを使用してコンテンツ113内にコード化されるかまたは確実に記憶した使用条件519内にコード化される。エンドユーザ装置109上で実行されるエンドユーザ・プレーヤ・アプリケーション195は、コンテンツ113内にコード化されたストア使用条件519が執行されることを保証する。

【0108】コンテンツ113が音楽である実施形態の場合のストア使用条件519の例を以下に示す。

- ・ 歌曲は記録可能である。
- ・ 歌曲はn回再生可能である。

【0109】C. セキュア・コンテナのフローおよび処理の概要

メタデータSC620は、コンテンツ・プロバイダ101によって構築され、歌曲などのコンテンツ113の項目を定義するために使用する。コンテンツ113のサイズは通常、電子デジタル・コンテンツ・ストア103とエンドユーザが記述メタデータにアクセスするためにだけそのコンテナを効率よくダウンロードするには大きすぎるので、コンテンツ113自体はこのようなSC内に含まれない。むしろ、SCはコンテンツ113を指し示すための外部URL（ユニフォーム・リソース・ロケータ）を含む。また、SCはコンテンツ113に関する記述情報と、歌曲コンテンツ113の場合は音楽用のCDカバー・アートまたはデジタル・オーディオ・クリップあるいはその両方などのその他の関連データを提供するメタデータも含む。

【0110】電子デジタル・コンテンツ・ストア103は、それに関する認可を受けているメタデータSC620をダウンロードし、オファーSC641を構築する。要するに、オファーSC641は、電子デジタル・コンテンツ・ストア103が含まれた追加情報とともにメタデータSC620からの全パーツの一部とBOMからなる。オファーSC641が構築されると、オファーSC641用の新しいBOMが作成される。また、電子デジタル・コンテンツ・ストア103は、エンドユーザが通常、コンテンツ113を購入できるように、それ

からメタデータ情報を抽出することにより、メタデータSC620を使用して、エンドユーザにコンテンツ113の記述を提示するHTMLページをそのウェブ・サイト上に構築する。

【0111】電子デジタル・コンテンツ・ストア103によって追加されるオファーSC641内の情報は通常、メタデータSC620に指定される使用条件517と、ストアのロゴのグラフィック画像ファイルやストアのウェブ・サイトへのURLなどのプロモーション・データの選択を狭くするためのものである。メタデータSC620内のオファーSC641のテンプレートは、オファーSC641内で電子デジタル・コンテンツ・ストア103がどの情報を指定変更できるか、電子デジタル・コンテンツ・ストア103がどの追加情報を必要とするか、ならびに埋込みメタデータSC620内にどのパーツが保持されるかを示す。

【0112】エンドユーザが電子デジタル・コンテンツ・ストア103からコンテンツ113を購入することを決定すると、オファーSC641がトランザクションSC640に含まれる。電子デジタル・コンテンツ・ストア103は、トランザクションSC640を構築し、購入するコンテンツ113の各項目ごとにオファーSC641を含め、それをエンドユーザ装置109に伝送する。エンドユーザ装置109は、トランザクションSC640を受け取り、トランザクションSC640と含まれるオファーSC641の完全性を妥当性検査する。

【0113】オーダSC650は、購入するコンテンツ113の各項目ごとにエンドユーザ装置109によって構築される。オファーSC641からの情報と、トランザクションSC640からの情報と、エンドユーザ装置109の構成ファイルからの情報が含まれる。オーダSC650は一度に1つずつクリアリング・ハウス105に送られる。オーダSC650がメタデータSC620用のBOM内のレコードの1つとして含まれるクリアリング・ハウス105のURLも同じくオファーSC641に含まれる。

【0114】クリアリング・ハウス105は、オーダSC650を妥当性検査して処理し、ライセンス・ウォーターマーク527に対して必要で、かつ購入したコンテンツ113にアクセスするために必要なあらゆるものをエンドユーザ装置109に提供する。クリアリング・ハウス105の機能の1つは、オファーSC641からのウォーターマーク命令とコンテンツSC630からのコンテンツ113を暗号化解除するのに必要な対称キー623を暗号化解除することである。暗号化対称キー623のレコードは、実際には、実際の暗号化対称キー623以上のものを含んでいる。暗号化を実行する前に、コンテンツ・プロバイダ101は任意選択でその名前を実際の対称キー623に付加することができる。対称キー62

3とともにコンテンツ・プロバイダ101の名前が暗号化されているので、合法的SCからそれ自身のメタデータSC620とコンテンツSC630を構築した著作権侵害コンテンツ・プロバイダ101から保護される。クリアリング・ハウス105は、対称キー623とともに暗号化されたコンテンツ・プロバイダ101の名前がSC証書内のコンテンツ・プロバイダ101の名前と一致することを検証する。

【0115】クリアリング・ハウス105によってウォータマーク命令に対して何らかの変更を行う必要がある場合、クリアリング・ハウス105は対称キー623を暗号化解除し、次にウォータマーク命令を変更し、新しい対称キー623を使用してそれをもう一度暗号化する。その後、対称キー623は、エンドユーザ装置109の公開キー661を使用して再暗号化される。また、クリアリング・ハウス105は、SC内の他の対称キー623も暗号化解除し、エンドユーザ装置109の公開キー661でそれをもう一度暗号化する。クリアリング・ハウス105は、新たに暗号化した対称キー623と更新したウォータマーク命令を含むライセンスSC660を構築し、オーダSC650に応答してそれをエンドユーザ装置109に送る。オーダSC650の処理が正常に完了しない場合、クリアリング・ハウス105は認可プロセスの失敗を報告するHTMLページまたは同等のものをエンドユーザ装置109に返す。

【0116】ライセンスSC660は、コンテンツ113の項目にアクセスするために必要なあらゆるものをエンドユーザ装置109に提供する。エンドユーザ装置109はコンテンツ・ホスト・サイト111から適切なコンテンツSC630を要求する。コンテンツSC630は、コンテンツ・プロバイダ101によって構築され、暗号化コンテンツ113とメタデータ・パーツを含む。エンドユーザ・プレーヤ・アプリケーション195は、ライセンスSC660からの対称キー623を使用して、コンテンツ113、メタデータ、ウォータマーク命令を暗号化解除する。次に、ウォータマーク命令はコンテンツ113内に添付され、コンテンツ113はスクランブルされてエンドユーザ装置109に記憶される。

【0117】D. メタデータ・セキュア・コンテナ620のフォーマット

以下の表はメタデータSC620に含まれるパーツを示している。パーツ列の各ボックスは、BOMとともにSCに含まれる個別のオブジェクトである（[]という文字で囲まれたパーツ名は除く）。BOMはSCに含まれる各パーツのレコードを含む。パーツ存在列はそのパーツ自体が実際にSCに含まれているかどうかを示し、ダイジェスト列はそのパーツについてメッセージ・ダイジェストが計算されるかどうかを示す。元のBOM全体は伝播されるが、（関連テンプレートによって決定されるように）あるSCが他のSCに含まれるとパーツによっては伝播されない場合がある。これは、元のSC内のデジタル・シグニチャを検証するためにクリアリング・ハウス105がBOM全体を必要とするためである。

【0118】以下の表のキー記述パーツ列は、SCのキー記述パーツに含まれるレコードを定義するものである。キー記述パーツ内のレコードは、そのSC内のパーツまたは他のSC内のパーツを暗号化するために使用した暗号化キーおよびアルゴリズムに関する情報を定義する。各レコードは、暗号化パーツ名と、必要であれば、その暗号化パーツを含む他のSCを指し示すURLとを含む。結果名列は、それが暗号化解除された後でそのパーツに割り当てられる名前を定義する。暗号化アルゴリズム列は、そのパーツを暗号化するために使用した暗号化アルゴリズムを定義する。キーID/暗号化キー列は、そのパーツを暗号化するために使用した暗号化キーの識別名またはそのパーツを暗号化するために使用した暗号化対称キー623のビット・ストリングのベース64コード化のいずれかを定義する。対称キー・アルゴリズム列は、前の列が暗号化対称キー623であるときに対称キー623を暗号化するために使用した暗号化アルゴリズムを定義する任意選択のパラメータである。対称キーID列は、キーID/暗号化キー列が暗号化対称キー623であるときに対称キー623を暗号化するために使用した暗号化キーの識別名である。

【0119】

【表3】

BOM	
ハーフ	タグ
[コンテンツURL]	SCA-ジョ
[メタデータURL]	SC ID
	SCタイプ
	SC発行者
	日付
	満了日
	クリアリング・ハウスURL
	タグ・リスト・アルゴリズムID
	キー・ID・アルゴリズムID
コンテンツID	有
メタデータ	有
使用条件	有
SCテンプレート	有
ウォーターマーク命令	有
キー記述ハーフ	有
クリアリング・ハウス証書	有
証書	有
	キー・ID・アルゴリズムID

結果名	暗号化7 アルゴリズム	キーID/ 暗号化キー	対称キー アルゴリズム	対称キーID
出力ハーフ	RC4	暗号化対称キー	RSA	公開キー
出力ハーフ	RC4	暗号化対称キー	RSA	公開キー

出力ハーフ	RC4	暗号化対称キー	RSA	公開キー
-------	-----	---------	-----	------

【0120】上記のメタデータSCの表で使用する用語について以下に説明する。

・ [コンテンツURL] - キー記述パーツのレコード内のパラメータ。これは、コンテンツSC630内にあってこのメタデータSC620に関連する暗号化コンテンツ113を指し示すURLである。メタデータSC620自体は暗号化コンテンツ113を含まない。

・ [メタデータURL] - キー記述パーツのレコード内のパラメータ。これは、コンテンツSC630内にあってこのメタデータSC620に関連する暗号化メタデータを指し示すURLである。メタデータSC620自体は暗号化メタデータを含まない。

・ コンテンツID - コンテンツ113の項目に割り当てられた固有のIDを定義するパーツ。メタデータSC620がコンテンツ113の複数の項目を参照する場合、このパーツ内に複数のコンテンツIDが含まれる。

・ メタデータ - 歌曲の場合はアーティスト名およびCDカバー・アートなどのコンテンツ113の項目に関する情報を含むパーツ。複数のメタデータ・パーツが存在する可能性があり、そのうちの一部分が暗号化可能である。メタデータ・パーツの内部構造はそこに含まれるメタデータのタイプに依存する。

・ 使用条件 - コンテンツ113の使用のためにエンドユーザに課せられる使用オプション、規則、制限を記述する情報を含むパーツ。

・ SCテンプレート - オファー、オード、ライセンスの各SC660を構築するための必須情報および任意選択情報を記述するテンプレートを定義するパーツ。

・ ウォータマーク命令 - コンテンツ113内でウォータマークを実施するための暗号化命令およびパラメータを含むパーツ。ウォータマーク命令は、クリアリ

グ・ハウス105によって変更可能であり、ライセンスSC660内でエンドユーザ装置109に返すことができる。ウォータマーク命令を暗号化するために使用した暗号化アルゴリズム、ウォータマーク命令を暗号化解除するときに使用する出力パーツ名、ウォータマーク命令を暗号化するために使用した暗号化対称キー623のビット・ストリングのベース64コード化、対称キー623を暗号化するために使用した暗号化アルゴリズム、対称キー623を暗号化解除するために必要な公開キーの識別名を定義するレコードがキー記述パーツ内に存在する。

・ クリアリング・ハウス証書 - クリアリング・ハウス105のサイン付き公開キー621を含む、証明機関からまたはクリアリング・ハウス105からの証書。複数の証書が存在する可能性があり、その場合、階層レベル構造が使用され、二番目に高いレベルの証書をオープンするための公開キーを含む最高レベルの証書が届けられ、それはクリアリング・ハウス105の公開キー621を含む。

・ 証書 - SCを作成したエンティティのサイン付き公開キー621を含む、証明機関からまたはクリアリング・ハウス105からの証書。複数の証書が存在する可能性があり、その場合、階層レベル構造を使用し、SC作成者の公開キー621を含む最低レベルの証書に達するまで、最高レベルの証書は次のレベルの証書などをオープンするための公開キーを含む。

・ SCバージョン - SCバック・ツールによってSCに割り当てられたバージョン番号。

・ SC ID - SCを作成したエンティティによってそのSCに割り当てられた固有のID。

・ SCタイプ - SCのタイプ（たとえば、メタデータ、オファー、オードなど）を示す。

- ・ SC発行者 - SCを作成したエンティティを示す。
- ・ 作成日 - SCが作成された日付。
- ・ 満了日 - SCが満期になり、もはや有効ではなくなる日付。
- ・ クリアリング・ハウスURL - コンテンツ113にアクセスするための適正な認可を得るためにエンドユーザ・ブレーヤ・アプリケーション195が対話しなければならないクリアリング・ハウス105のアドレス。
- ・ ダイジェスト・アルゴリズムID - パーツのダイジェストを計算するために使用するアルゴリズムの識別子。
- ・ デジタル・シグニチャ・アルゴリズムID - 連結パーツ・ダイジェストのダイジェストを暗号化するために使用するアルゴリズムの識別子。この暗号化値はデジタル・シグニチャである。
- ・ デジタル・シグニチャ - SCを作成したエンティティの公開キーで暗号化した連結パーツ・ダイジェストのダイジェスト。

- ・ 出力パーツ - 暗号化パーツを暗号化解除するとき出力パーツに割り当てる名前。
 - ・ RSAおよびRC4 - 対称キー623とデータ・パーツを暗号化するために使用するデフォルト暗号化アルゴリズム。
 - ・ 暗号化対称キー - 暗号化解除したときにSCパーツを暗号化解除するために使用する暗号化キー・ビット・ストリングのベース64コード化。
 - ・ CH公開キー - クリアリング・ハウス105の公開キー621を使用してそのデータを暗号化したことを示す識別子。
- 【0121】E. オファー・セキュア・コンテナ641のフォーマット
- 以下の表はオファーSC641に含まれるパーツを示している。メタデータ・パーツの一部を除くパーツと、メタデータSC620からのBOMもオファーSC641に含まれる。
- 【0122】
- 【表4】

51

ハ-ツ BOM

ハ-ツ存在 タ-イシ-エスト 結果名 暗号化7 アルゴリズム キ-記述ハ-ツ キ-ID/ 暗号化キ- 対称キ-7 アルゴリズム 対称キ-ID

メタ-タSCハ-ツ

出力ハ-ツ	RC4	暗号化対称キ-	RSA	CH公開キ-
出力ハ-ツ	RC4	暗号化対称キ-	RSA	CH公開キ-

コンテンツURL	SCハ-ツ-シ-37	
メタ-タURL	SC ID	
	SCタ-イ7	
	SC発行者	
	日付	
	満了日	
	クリアリング・ハウスURL	
	タ-イシ-エスト7アルゴリズムAID	
	デ-イシ-タ-ル・シ-ク・ニ-チャ7アルゴリズムAID	
コンテンツID	有	有
メタ-タ	一部	有
使用条件	有	有
SCテンプレート	有	有
ウォーターマーク命令	有	有
キ-記述ハ-ツ	有	有
クリアリング・ハウス証書	有	無
証書	有	無
	デ-イシ-タ-ル・シ-ク・ニ-チャ	

出力ハ-ツ RC4 暗号化対称キ- RSA CH公開キ-

477-SCハ-ツ

SCハ-ツ-シ-37		
SC ID		
SCタ-イ7		
SC発行者		
日付		
満了日		
タ-イシ-エスト7アルゴリズムAID		
デ-イシ-タ-ル・シ-ク・ニ-チャ7アルゴリズムAID		
メタ-タSC BOM	有	有
追加および指定変更フィールド	有	有
電子デ-イシ-タ-ル・コンテンツ・ストア証書	有	無
証書	有	無
	デ-イシ-タ-ル・シ-ク・ニ-チャ	

【0123】上記のオフーSC641で使用する用語のうち、他のSCに関して前述していない用語について以下に説明する。

・ メタデータSCBOM - 元のメタデータSC620からのBOM。オフーSC641のBOM内のレコードはメタデータSC620のBOMのダイジェストを含む。

・ 追加および指定変更フィールド - 電子デジタル・コンテンツ・ストア103によって指定変更された使用条件情報。受け取ったSCテンプレートによりクリアリング・ハウス105がこの情報を妥当性検査し、電子デジタル・コンテンツ・ストア103が指定変更するものはいずれもその認可の範囲内であることを確認する。

・ 電子デジタル・コンテンツ・ストア証書 - クリアリング・ハウス105によって電子デジタル・コンテンツ・ストア103に提供され、その秘密キーを使用してクリアリング・ハウス105がサインした証書。この証書は、電子デジタル・コンテンツ・ストア10

3がコンテンツ113の有効な配布者であることを検証するためにエンドユーザ・プレーヤ・アプリケーション195が使用する。エンドユーザ・プレーヤ・アプリケーション195とクリアリング・ハウス105は、クリアリング・ハウス105の公開キー621で証書のシグニチャを暗号化解除することにより、電子デジタル・コンテンツ・ストア103が認可配布者であることを検証することができる。エンドユーザ・プレーヤ・アプリケーション195は、それがインストール時にその初期設定の一部として受け取るクリアリング・ハウス105の公開キー621のローカル・コピーを保持する。

【0124】F. トランザクション・セキュア・コンテンツ640のフォーマット

以下の表はトランザクションSC640に含まれるパーツならびにそのBOMおよびキー記述パーツを示している。

【0125】

【表5】

BOM		結果名			
BOM		暗号化アルゴリズム	キー記述ハッシュ キーID/暗号化キー	対称キー アルゴリズム	対称キーID
トランザクションID	有	有	出力ハッシュ	RSA	CH公開キー
エンドユーザID	有	有	出力ハッシュ	RSA	CH公開キー
エンドユーザの公開キー	有	有			
オフーSC	有	有			
コンテンツ使用の選択	有	有			
表示用HTML	有	有			
キー記述ハッシュ	有	有			
電子デジタル・コンテンツストア証明書	有	無			
デジタル・シグニチャ					

【0126】上記のトランザクションSC640で使用する用語のうち、他のSCに関して前述していない用語について以下に説明する。

・ トランザクションID535 - トランザクションを明確に識別するために電子デジタル・コンテンツ・ストア103によって割り当てられるID。

・ エンドユーザID - エンドユーザが購入選択を行い、クレジット・カード情報を提供したときに電子デジタル・コンテンツ・ストア103が取得するエンドユーザの識別名。

・ エンドユーザの公開キー - 対称キー623を再暗号化するためにクリアリング・ハウス105が使用するエンドユーザの公開キー661。エンドユーザの公開キー661は購入トランザクション中に電子デジタル・コンテンツ・ストア103に伝送される。

・ オfferSC - 購入されたコンテンツ113の項目に関するオfferSC641。

・ コンテンツ使用の選択 - エンドユーザが購入するコンテンツ113の各項目ごとの使用条件のアレ。

各オfferSC641ごとに1つの項目が存在する。
・ 表示用HTML - トランザクションSC640を受け取った後またはエンドユーザ装置109とクリアリング・ハウス105との対話中にエンドユーザ・ブレイヤ・アプリケーション195がインターネット・ブラウザのウィンドウ内に表示する1つまたは複数のHTMLページ。

【0127】エンドユーザ装置109がトランザクションSC640を受け取った場合、SCの完全性と信憑性を検証するために以下のステップを実行することができる。

1. クリアリング・ハウス105の公開キー621を使用して電子デジタル・コンテンツ・ストア103の証書の完全性を検証する。クリアリング・ハウス105の公開キー621は、そのインストール・プロセス中にエンドユーザ・ブレイヤ・アプリケーション195の初期設定の一部として受け取られた後、エンドユーザ装置109に記憶されている。

2. 電子デジタル・コンテンツ・ストア103の証書からの公開キーを使用してSCのデジタル・シグニチャ643を検証する。

3. SCパーツのハッシュを検証する。

4. トランザクションSC640に含まれる各オfferSC641の完全性と信憑性を検証する。

【0128】G. オーダ・セキュア・コンテナ650のフォーマット

以下の表はオーダSC650に含まれるパーツならびにそのBOMおよびキー記述パーツを示している。これらのパーツは、暗号化解除および検証のためにクリアリング・ハウス105に情報を提供するか、またはクリアリング・ハウス105によって妥当性検査される。オfferSC641からのパーツおよびBOMもオーダSC650に含まれる。メタデータSCのBOMのパーツ存在列内の一部という文字列は、これらのパーツの一部がオーダSC650に含まれないことを示している。クリアリング・ハウス105がメタデータSC620とそのパーツの完全性を妥当性検査できるように何らかの変更を行わずに、メタデータSC620からのBOMも含まれる。

【0129】

【表6】

BOM

結果名

キ-記述ハ°-7

キ-ID/	対称キ-
暗号化キ-	7ルコリス*ム

对称4-ID

出力ハッシュ	RC4	暗号化対称キー	RSA	CH公開キー
出力ハッシュ	RC4	暗号化対称キー	RSA	CH公開キー

SCA-シヨ	
SC ID	
SCタイプ	
SC発行者	
日付	
満了日	
クリアリングハウスURL	
タインストアスコリスID	
ティンストアシグニチャ	
アスコリスID	
有	有
一部	有
有	有
有	有
有	有
有	有
有	有
有	無
有	無
ティンストアシグニチャ	

出力ハッシュ	RC4	暗号化対称キー	RSA	CH公開キー
--------	-----	---------	-----	--------

-----777-SCA-シヨ-----

SCA-シヨ	
SC ID	
SCタイプ	
SC発行者	
日付	
満了日	
タインストアスコリスID	
ティンストアシグニチャ	
アスコリスID	
有	有
有	有
有	無
有	無
ティンストアシグニチャ	

メタデータSC BOM
追加および指定変更フィールド
電子ティンストアシグニチャ
コンテンツストア証書
証書

【表7】

(表6の続き)

トランザクションSCA'-ウ

SCA'-ジ'ヨ
SC ID
SC発行
SC発行者
日付
満了日
ダイジェスト・アロジ'リス'ΔID
デジタル・シグ'ニチャ'アロジ'リス'ΔID

出力ハ'-ウ	RSA	CH公開キ-
出力ハ'-ウ	RSA	CH公開キ-

トランザクションID
イント'-サ'ID
イント'-サ'の公開キ-
オフ'-SC
コンテンツ使用の選択
表示用HTML
キー記述ハ'-ウ
電子デ'イ'タル・コンテンツストア証書

デジタル・シグ'ニチャ'

注文SCA'-ウ

SCA'-ジ'ヨ
SC ID
SC発行
SC発行者
日付
満了日
ダイジェスト・アロジ'リス'ΔID
デジタル・シグ'ニチャ'アロジ'リス'ΔID

出力ハ'-ウ	RSA	CH公開キ-
--------	-----	--------

オフ'-SC BOM
トランザクションSC BOM
暗号化クレジット・カード情報
キー記述ハ'-ウ

デジタル・シグ'ニチャ'

【0130】上記のオーダSC650で使用する用語のうち、他のSCに関して前述していない用語について以下に説明する。

・ トランザクションSCBOM - 元のトランザクションSC640内のBOM。オーダSC650のBOM内のレコードはトランザクションSC640のBOMのダイジェストを含む。

・ 暗号化クレジット・カード情報 - その購入をクレジット・カードまたはデビット・カードに請求するために使用する、エンドユーザからの任意選択の暗号化情報。この情報は、オフ'-SC641を作成した電子デジタル・コンテンツ・ストア103が顧客請求を処理しないときに必要になり、その場合、クリアリング・ハウス105がその請求を処理することができる。

【0131】H. ライセンス・セキュア・コンテナ660のフォーマット

以下の表はライセンスSC660に含まれるパーツならびにそのBOMを示している。キー記述パーツに示すように、ウォータマーク命令、コンテンツ113、コンテンツ113のメタデータを暗号化解除するために必要な対称キー623は、エンドユーザの公開キー661を使用してクリアリング・ハウス105によって再暗号化されている。エンドユーザ装置109がライセンスSC660を受け取ると、それは対称キー623を暗号化解除し、それらを使用してライセンスSC660およびコンテンツSC630からの暗号化パーツにアクセスする。

【0132】

【表8】

59

BOM	
ハ-ツ存在	タ-イ'エ'スト
[コンテンツURL]	
[メタ-タURL]	
SCA'-ジ'ョ'ン	
SC ID	
SC'イ'フ'	
SC発行者	
日付	
満了日	
タ'イ'エ'スト・アル'コ'リス'ΔID	
デ'イ'グ'ル・シ'ク'ニ'ヤ	
アル'コ'リス'ΔID	
コンテンツID	有
使用条件	有
トラン'ク'シ'ョ'ン・デ-タ	有
ウ-タ-マ-タ命令	有
キ-記述ハ-ツ	有
証書	有
デ'イ'グ'ル・シ'ク'ニ'ヤ	

結果名	略号化7 アル'コ'リス'Δ	キ-ID/ 暗号化キ-	対称キ- アル'コ'リス'Δ	対称キ-ID
出力ハ-ツ	RC4	暗号化対称キ-	RSA	EU公開キ-
出力ハ-ツ	RC4	暗号化対称キ-	RSA	EU公開キ-

出力ハ-ツ	RC4	暗号化対称キ-	RSA	EU公開キ-
-------	-----	---------	-----	--------

【0133】上記のライセンスSC660で使用する用語のうち、他のSCに関して前述していない用語について以下に説明する。

・ EU公開キー - エンドユーザの公開キー661 20
を使用してそのデータを暗号化したことを示す識別子。

・ オータSC650のID - オータSC650のBOMから取得したSCのID。

・ 証書撤回リスト - クリアリング・ハウス105によって前に発行され、サインされたが、もはや有効とは見なされない証書IDの任意選択のリスト。撤回リストに含まれる証書によって検証可能なシグニチャを有するSCは無効SCである。エンドユーザ・プレーヤ・アプリケーション195はクリアリング・ハウス105の証書撤回リストのコピーをエンドユーザ装置109に記憶する。撤回リストを受け取ると、エンドユーザ・プレーヤ・アプリケーション195は、新しいリストがより最新のものである場合、そのローカル・コピーを置き換える。撤回リストは、どのリストが最も最新ものであるかを判定するために、バージョン番号またはタイム・スタンプ（あるいはその両方）を含む。

【0134】I. コンテンツ・セキュア・コンテナのフォーマット

以下の表はコンテンツSC630に含まれるパーツならびにそのBOMを示している。

【0135】

【表9】

ハ-ツ

BOM	
ハ-ツ存在	タ-イ'エ'スト
SCA'-ジ'ョ'ン	
SC ID	
SC'イ'フ'	
SC発行者	
日付	
満了日	
クリ'リ'ク'ハ'ウ'ス105URL	
タ'イ'エ'スト・アル'コ'リス'ΔID	
デ'イ'グ'ル・シ'ク'ニ'ヤ	
アル'コ'リス'ΔID	
コンテンツID	有
暗号化コンテンツ	有
暗号化メタ-タ	有
メタ-タ	有
証書	有
デ'イ'グ'ル・シ'ク'ニ'ヤ	

【0136】上記のコンテンツSC630で使用する用語のうち、他のSCに関して前述していない用語について以下に説明する。

・ 暗号化コンテンツ - 対称キー623を使用してコンテンツ・プロバイダ101によって暗号化されたコンテンツ113。

・ 暗号化メタデータ - コンテンツ113に関連するメタデータのうち、対称キー623を使用してコンテンツ・プロバイダ101によって暗号化されたメタデータ。

【0137】暗号化パーツを暗号化解除するために必要なキーはクリアリング・ハウス105で構築されたライセンスSC660内にあるので、コンテンツSC630にはキー記述パーツは一切含まれない。

【0138】VI. セキュア・コンテナのバックおよびアンバック

A. 概要

SCのバックは、指定のパーツのすべてを使ってSCを作成するために複数または単一ステップ・プロセスで呼び出すことができ、API（アプリケーション・プログ

ラミング・インタフェース)を備えた32ビットのWindowsプログラムである。SCのバック151、152、153は、コンテンツ・プロバイダ101、クリアリング・ハウス105、電子デジタル・コンテンツ・ストア103、SCのバックを必要とするその他のサイトでWindowsプログラムをサポートする様々なハードウェア・プラットフォームである。BOMと、必要であればキー記述パーツが作成され、SCに含まれる。1組のバックAPIにより、呼出し側は、BOMおよびキー記述パーツ内のレコードを生成し、SCにパーツを含めるのに必要な情報を指定することができる。パーツおよび対称キー623の暗号化ならびにダイジェストおよびデジタル・シグニチャの計算もバックによって実行される。バックがサポートする暗号化およびダイジェスト・アルゴリズムはバック・コードに含まれるかまたは外部インタフェースを介して呼び出される。

【0139】SCを構築するためのバックへのインタフェースは1つのAPIによって行われ、そのAPIは以下のパラメータを入力として受け入れる。

- ・ 連結構造のバッファを指し示すポインタ。バッファ内の各構造は、バックへのコマンドであり、そのコマンドを実行するのに必要な情報を伴う。バック・コマンドとしては、関連BOMレコードを備えたSCにパーツを追加すること、BOMにレコードを追加すること、キー記述パーツにレコードを追加することを含む。

- ・ 上記のバッファに含まれる連結構造の数を示す値。

- ・ BOMパーツの名前および位置。

- ・ 各ビットが定義済みフラグまたは今後の使用のための予約済みフラグである値。現在、以下のフラグが定義されている。

- ー バッファ内のすべての構造が処理された後でSCのすべてのパーツをまとめてバンドルして単一ファイルにしなければならないかどうかに関する表示。全パーツを単一オブジェクトにバンドルすることは、SCを構築するときに実行する最後のステップである。

- ー デジタル・シグニチャがBOMパーツから省略されているかどうかに関する表示。このフラグが設定されていない場合、SCが単一オブジェクトにバンドルされる直前にデジタル・シグニチャが計算される。

【0140】代替実施形態では、SCを構築するためのバックへのインタフェースは複数APIによって行われ、そのAPIは以下のパラメータを入力として受け入れる。

- ・ まず、SCのBOMパーツ内でIPレコードとして示されるSCの設定を初期設定するために使用する情報からなる構造を指し示すポインタとして、BOMパーツに使用するための名前と、追加されるパーツを探すためのデフォルト位置と、フラグ値とを渡すことにより、素材一覧表(BOM)パーツを作成するためにAPIが呼び出される。このAPIは、後続バックAPIで使用する

るSCハンドルを返す。

- ・ このバックは、SCにパーツが追加されるときに必ず使用するAPIを有する。このAPIは、前のバックAPIから事前に返されたSCハンドルと、追加されるパーツに関する情報からなる構造を指し示すポインタと、フラグ値とを受け入れる。追加されるパーツに関する情報としては、そのパーツの名前および位置、BOM内でそのパーツに使用するための名前、追加されるパーツのタイプ、そのパーツ用のハッシュ値、フラグなどを含む。

- ・ すべてのパーツがSCに追加された後で、BOMパーツを含むすべてのパーツを、通常はファイルである単一SCオブジェクトにバックするためにバックAPIが呼び出される。このAPIは、前のバックAPIから事前に返されたSCハンドルと、バックしたSCに使用するための名前と、そのSCにサインするための情報を備えた構造を指し示すポインタと、フラグ値とを受け入れる。

【0141】バックまたはバックを呼び出すエンティティは、SCテンプレートを使用してSCを構築することができる。SCテンプレートは、構築中のSCで必要なパーツおよびレコードを定義する情報を有する。また、テンプレートは、暗号化対称キー623および暗号化パーツに使用するための暗号化方法およびキー参照も定義することができる。

【0142】バックは、SCをアンパックするために使用するAPIを有する。SCのアンパックは、SCを取得し、それを個々のパーツに分離するプロセスである。その後、そのバックを呼び出して、SCからアンパックされた暗号化パーツのいずれかを暗号化解除することができる。

【0143】B. 素材一覧表(BOM)パーツ
BOMパーツは、SCを構築するときにバックによって作成される。BOMは、SCとそのSCに含まれるパーツに関する情報のレコードを含むテキスト・ファイルである。BOM内の各レコードは単一行上にあり、新しいレコードの開始は新しい行が示す。通常、BOMは、各パーツのダイジェストと、そのSCの信憑性および完全性を妥当性検査するために使用可能なデジタル・シグニチャとを含む。

【0144】BOM内のレコード・タイプは以下の通りである。

IP IPレコードは、そのSCに関係する1組の名前=値の対を含む。SCの特定のプロパティのために以下の名前が予約されている。

V major.minor.fix

VプロパティはSCのバージョンを指定する。これは、SCが作成されたときのSC仕様のバージョン番号である。後続の文字列は、major.minor.fixという形式でなければならない、major、minor、fixはそれぞれメジャー

・リリース番号、マイナ・リリース番号、修正レベルである。

ID value

IDプロパティは、このSCを作成するエンティティがこの特定のSCに割り当てる固有の値である。この値のフォーマットは本書の今後のバージョンで定義される。

T value

TプロパティはSCのタイプを指定し、以下のいずれか1つでなければならない。

ORD - オーダSC650

OFF - オファーSC641

LIC - ライセンスSC

TRA - トランザクションSC640

MET - メタデータSC620

CON - コンテンツSC630

A value

AプロパティはSCの作成者または発行者を識別する。作成者／発行者のアイデンティティは、明白なものであるかまたはクリアリング・ハウス105に登録しなければならない。

D value

Dプロパティは、SCが作成された日付と、任意選択で時刻を識別する。この値は、年／月／日@時：分：秒、小数秒（時間帯）を表すyyyy/mm/dd[@hh:mm[:ss[.fsec]][(TZ)]]という形式でなければならない。この値の任意選択部分は[]という文字で囲まれている。

E value

Eプロパティは、SCが満期になる日付と、任意選択で時刻を識別する。この値は、前に定義したDプロパティで使用するのと同じ形式でなければならない。満了日／時刻は、可能であれば必ず、クリアリング・ハウス105での日付／時刻と比較しなければならない。

CCURL value

CCURLプロパティはクリアリング・ハウス105のURLを識別する。この値は、有効な外部URLの形式でなければならない。

H value

Hプロパティは、SCに含まれるパーツ用のメッセージ・ダイジェストを計算するために使用したアルゴリズムを識別する。ダイジェスト・アルゴリズムの一例はMD5である。

D Dレコードは、パーツのタイプ、パーツの名前、パーツの（任意選択の）ダイジェスト、そのパーツがSCに含まれないという（任意選択の）表示を識別する情報を含むデータまたはパーツ項目レコードである。タイプ識別子の直後の一符号は、そのパーツがSCに含まれないことを示すために使用する。データまたはパーツ・レコードの予約済みタイプは以下の通りである。

K part_name [digest]

キー記述パーツを指定する。

W part_name [digest]

ウォーターマーク命令パーツを指定する。

C part_name [digest]

デジタル・シグニチャを妥当性検査するために使用する証書を指定する。

T part_name [digest]

使用条件パーツを指定する。

YF part_name [digest]

10 オファーSC641用のテンプレート・パーツを指定する。

YO part_name [digest]

オーダSC650用のテンプレート・パーツを指定する。

YL part_name [digest]

ライセンスSC660用のテンプレート・パーツを指定する。

ID part_name [digest]

参照中のコンテンツ113の項目のコンテンツ113のIDを指定する。

CH part_name [digest]

20 クリアリング・ハウス105の証書パーツを指定する。

SP part_name [digest]

電子デジタル・コンテンツ・ストア103の証書パーツを指定する。

B part_name [digest]

このSCに含まれるそのパーツまたはそのパーツのサブセットを有する他のSCのBOMパーツを指定する。

BP part_name sc_part_name [digest]

30 単一パーツとしてこのSCに含まれる他のSCのBOMパーツを指定する。sc_part_nameというパラメータは、このSCに含まれ、このBOMパートが定義するSCパーツの名前である。これと同一のBOMも、sc_part_nameパラメータによって定義されるSCに含まれる。

D part_name [digest]

データ（またはメタデータ）パーツを指定する。

S Sレコードは、SCのデジタル・シグニチャを定義するために使用するシグニチャ・レコードである。デジタル・シグニチャは以下のように指定される。

S key_identifier signature_string signature_algorithm

40 Sレコードは、シグニチャの暗号化キーを示すためのkey_identifierと、デジタル・シグニチャ・ビットストリングのベース64コード化であるsignature_stringと、ダイジェストを暗号化してデジタル・シグニチャを作成するために使用したsignature_algorithmとを含む。

【0145】C. キー記述パーツ

キー記述パーツは、SCの暗号化パーツの暗号化解除のために必要な暗号化キーに関する情報を提供するためにバックによって作成される。暗号化パーツは、構築中のSCに含まれる場合もあれば、構築中のSCが参照する

他のSCに含まれる場合もある。キー記述パーツは、暗号化キーと、その暗号化キーが使用されたパーツに関する情報のレコードを含むテキスト・ファイルである。キー記述パーツ内の各レコードは単一行上にあり、新しいレコードの開始は新しい行が示す。

【0146】以下のレコード・タイプは、キー記述パーツ内で使用され、以下のように定義される。

K encrypted_part_name; result_part_name; part_encryption_algorithm_identifier; public_key_identifier; key_encryption_algorithm; encrypted_symmetric_key

Kレコードは、このSCに含まれる可能性があるかまたはこのレコードが参照する他のSCに含まれる可能性のある暗号化パーツを指定する。encrypted_part_nameは、このSC内のパーツの名前かまたは他のSC内の暗号化パーツの名前を指し示すURLのいずれかである。result_part_nameは、暗号化解除したパーツに与えられる名前である。part_encryption_algorithm_identifierは、そのパーツを暗号化するために使用した暗号化アルゴリズムを示す。public_key_identifierは、対称キー623を暗号化するために使用したキーの識別子である。key_encryption_algorithmは、対称キー623を暗号化するために使用した暗号化アルゴリズムを示す。encrypted_symmetric_keyは、そのパーツを暗号化するために使用した暗号化対称キー623のビット・ストリングのベース64コード化である。

【0147】VII. クリアリング・ハウス105

A. 概要

クリアリング・ハウス105は、セキュア・デジタル・コンテンツ電子配布システム100の権利管理機能を担当する。クリアリング・ハウス105の機能としては、電子デジタル・コンテンツ・ストア103を使用可能にすること、コンテンツ113に対する権利を検証すること、購入トランザクションおよび関連情報の完全性および信憑性を妥当性検査すること、コンテンツ暗号化キーまたは対称キー623をエンドユーザ装置109に配布すること、これらのキーの配布を追跡すること、電子デジタル・コンテンツ・ストア103およびコンテンツ・プロバイダ101にトランザクション要約を報告することを含む。コンテンツ暗号化キーは、通常は認可電子デジタル・コンテンツ・ストア103からの購入トランザクションによってエンドユーザ装置がそれに関する権利を取得したコンテンツ113をロック解除するためにエンドユーザ装置109が使用する。コンテンツ暗号化キーがエンドユーザ装置109に送られる前に、クリアリング・ハウス105は、検証プロセスを経て、コンテンツ113を販売するエンティティの信憑性と、エンドユーザ装置109がそのコンテンツ113に対して持っている権利を妥当性検査する。これはSC分析ツール185と呼ばれる。一部の構成では、クリアリ

ング・ハウス105は、クレジット・カード認証および請求という電子デジタル・コンテンツ・ストア103の機能を実行するシステムをクリアリング・ハウス105に併置することにより、購入したコンテンツ113の金融決済も処理することができる。クリアリング・ハウス105では、ICVerifyおよびTaxwareなどのOEMパッケージを使用して、クレジット・カードの処理および地域の売上税を処理する。

【0148】電子デジタル・コンテンツ・ストアの実施形態

セキュア・デジタル・コンテンツ電子配布システム100においてコンテンツ113の販売者として関与することを希望する電子デジタル・コンテンツ・ストア103は、セキュア・デジタル・コンテンツ電子配布システム100にコンテンツ113を提供するデジタル・コンテンツ・プロバイダ101の1つまたは複数に対して要求を行う。2人の当事者が合意に達する限り、要求を行うための決定的なプロセスはまったくない。電子デジタル・コンテンツ・ストア103がそのコンテンツ113を販売できるようにすることをたとえばソニー、タイムワーナーなどの音楽レーベルなどのデジタル・コンテンツ・レーベルが決定した後、クリアリング・ハウス105は通常はEメールを介して、電子デジタル・コンテンツ・ストア103をセキュア・デジタル・コンテンツ電子配布システム100に追加するという要求によって連絡を受ける。デジタル・コンテンツ・レーベルは、電子デジタル・コンテンツ・ストア103の名前と、クリアリング・ハウス105が電子デジタル・コンテンツ・ストア103用のデジタル証書を作成するために必要と思われるその他の情報を提供する。デジタル証書は、安全なやり方でデジタル・コンテンツ・レーベルによって電子デジタル・コンテンツ・ストア103に転送される。クリアリング・ハウス105は、それが割り当てたデジタル証書のデータベースを維持する。各証書は、バージョン番号、固有の通し番号、サイン・アルゴリズム、発行者の名前（たとえば、クリアリング・ハウス105の名前）、その証書が有効と見なされる期間、電子デジタル・コンテンツ・ストア103の名前、電子デジタル・コンテンツ・ストア103の公開キー、クリアリング・ハウス105の秘密キーを使用してサインした他の情報すべてのハッシュ・コードを含む。クリアリング・ハウス105の公開キー621を有するエンティティは、その証書を妥当性検査することができ、その後、証書からの公開キーを使用して妥当性検査可能なシグニチャが付いたSCは有効なSCであることが保証される。

【0149】電子デジタル・コンテンツ・ストア103は、クリアリング・ハウス105によって作成されたそのデジタル証書と、SCを処理するために必要なツ

ールをデジタル・コンテンツ・レーベルから受け取った後、エンドユーザが購入可能なコンテンツ113の提供を開始することができる。電子デジタル・コンテンツ・ストア103は、その証書とトランザクションSC640を含み、そのデジタル・シグニチャ643を使用してSCにサインする。エンドユーザ装置109は、まずデジタル証書撤回リストをチェックし、次にクリアリング・ハウス105の公開キー621を使用して電子デジタル・コンテンツ・ストア103用のデジタル証書内の情報を検証することにより、電子デジタル・コンテンツ・ストア103がセキュア・デジタル・コンテンツ電子配布システム100上でコンテンツ113の有効な配布者であることを検証する。デジタル証書撤回リストはクリアリング・ハウス105によって維持される。撤回リストは、クリアリング・ハウス105によって作成されるライセンスSC660のパーツの1つとして含めることができる。エンドユーザ装置109は、電子デジタル・コンテンツ・ストア103のデジタル証書妥当性検査の一部としてそれを使用できるように、エンドユーザ装置109上に撤回リストのコピーを保持する。エンドユーザ装置109は、ライセンスSC660を受け取ると、新しい撤回リストが含まれているかどうかを判定し、含まれている場合にはエンドユーザ装置109上のローカル撤回リストが更新される。

【0150】B. 権利管理処理

オーダSCの分析

エンドユーザがオファーSC641を含むトランザクションSC640を電子デジタル・コンテンツ・ストア103から受け取った後で、クリアリング・ハウス105はそのエンドユーザからオーダSC650を受け取る。オーダSC650は、コンテンツ113とその用途に関連する情報、コンテンツ113を販売する電子デジタル・コンテンツ・ストア103に関する情報、コンテンツ113を購入するエンドユーザに関する情報を含むパーツからなる。クリアリング・ハウス105は、オーダSC650内の情報の処理を開始する前に、まずSCが実際に有効であり、それが含むデータが決して破壊されていないことを保証するための何らかの処理を実行する。

【0151】妥当性検査

クリアリング・ハウス105は、デジタル・シグニチャを検証することにより、オーダSC650の妥当性検査を開始し、次にクリアリング・ハウス105はオーダSC650のパーツの完全性を検証する。デジタル・シグニチャを妥当性検査するために、まずクリアリング・ハウス105は、サイン付きの場合は含まれているサイン・エンティティの公開キー661を使用してシグニチャ自体のコンテンツ631を暗号化解除する。(サイン・エンティティは、コンテンツ・プロバイダ101、電子デジタル・コンテンツ・ストア103、エンドユ

ーザ装置109、またはそのいずれかの組合せにすることができよう。)次に、クリアリング・ハウス105は、SCの連結パーツ・ダイジェストのダイジェストを計算し、それをデジタル・シグニチャの暗号化解除したコンテンツ113と比較する。2つの値が一致する場合、デジタル・シグニチャは有効である。各パーツの完全性を検証するために、クリアリング・ハウス105は、そのパーツのダイジェストを計算し、それをBOM内のダイジェスト値と比較する。クリアリング・ハウス105は同じプロセスに従って、オーダSC650内に含まれるメタデータおよびオファーSC641の各パーツに関するデジタル・シグニチャおよびパーツ完全性を検証する。

【0152】また、トランザクションおよびオファーSC641のデジタル・シグニチャの検証のプロセスは、電子デジタル・コンテンツ・ストア103がセキュア・デジタル・コンテンツ電子配布システム100によって認可されていることも間接的に検証する。これは、クリアリング・ハウス105が証書の発行者であることに基づくものである。あるいは、クリアリング・ハウス105は、電子デジタル・コンテンツ・ストア103からの公開キーを使用してトランザクションSC640およびオファーSC641のデジタル・シグニチャを正常に検証できるだろうが、SCにサインしたエンティティが関連の秘密キーの所有権を有する場合に限る。秘密キーの所有権を有するのは電子デジタル・コンテンツ・ストア103だけである。ただし、クリアリング・ハウス105は電子デジタル・コンテンツ・ストア103のローカル・データベースを有する必要がないことに留意されたい。というのは、ストアはクリアリング・ハウスの公開キーを使用してトランザクションSC640およびオファーSC641の公開キーにサインするからである。

【0153】次に、エンドユーザが購入するコンテンツ113のストア使用条件519がメタデータSC620に設定された制限の範囲に含まれることを保証するために、その条件がクリアリング・ハウス105によって妥当性検査される。メタデータSC620がオーダSC650内に含まれることを想起されたい。

【0154】キー処理

暗号化対称キー623およびウォーターマーク命令の処理は、オーダSC650の信憑性および完全性チェック、電子デジタル・コンテンツ・ストア103の妥当性検査、ストア使用条件519の妥当性検査が正常に完了した後で、クリアリング・ハウス105によって行われる。オーダSC650のメタデータSC620部分は通常、クリアリング・ハウス105の公開キー621を使用して暗号化したキー記述パーツ内に位置する複数の対称キー623を有する。対称キー623の暗号化は、メタデータSC620が作成されたときにコンテンツ・ブ

ロバイダ101によって行われる。

【0155】1つの対称キー623はウォータマーク命令を暗号化解除するために使用し、残りの対称キーはコンテンツ113および任意の暗号化メタデータを暗号化解除するために使用する。コンテンツ113は単一歌曲またはCD上の歌曲の集合全体を表すことができるので、各歌曲ごとに異なる対称キー623を使用することができる。ウォータマーク命令はオーダSC650のメタデータSC620部分内に含まれる。コンテンツ113および暗号化メタデータはコンテンツ・ホスト・サイト111のコンテンツSC630内にある。コンテンツSC630内の暗号化コンテンツ113およびメタデータ・パーツのURLおよびパーツ名は、オーダSC650のメタデータSC620部分のキー記述パーツ内に含まれる。クリアリング・ハウス105はその秘密キーを使用して対称キー623を暗号化解除し、次にエンドユーザ装置109の公開キー661を使用してそのそれぞれを暗号化する。エンドユーザ装置109の公開キー661はオーダSC650から取り出される。新しい暗号化対称キー623は、クリアリング・ハウス105がエンドユーザ装置109に返すライセンスSC660のキー記述パーツに含まれる。

【0156】対称キー623の処理時間中、クリアリング・ハウス105はウォータマーク命令に変更を加えたいと希望する場合がある。そうである場合、クリアリング・ハウス105が対称キー623を暗号化解除した後、ウォータマーク命令が変更され、再暗号化される。新しいウォータマーク命令は、エンドユーザ装置109に返されるライセンスSC660内のパーツの1つとして含まれる。

【0157】オーダSC650のすべての処理が成功した場合、クリアリング・ハウス105はエンドユーザ装置109にライセンスSC660を返す。エンドユーザ装置109はライセンスSC660情報を使用してコンテンツSC630をダウンロードし、暗号化コンテンツ113およびメタデータにアクセスする。また、ウォータマーク命令もエンドユーザ装置109によって実行される。

【0158】クリアリング・ハウス105がオーダSC650を正常に処理できない場合、エンドユーザ装置109にHTMLページが返され、そのページがインターネット・ブラウザのウィンドウに表示される。そのHTMLページは、クリアリング・ハウス105がそのトランザクションを処理できなかった理由を示す。

【0159】代替実施形態では、ユーザがその販売について設定されたリリース日以前にコンテンツ113のコピーを購入した場合、対称キー623なしでライセンスSC660が返される。対称キー623を受け取るためにリリース日以降にライセンスSC660がクリアリング・ハウス105に返される。一例として、コンテンツ

・プロバイダ101は、ユーザが新しい歌曲のリリース日以前にその歌曲をダウンロードできるようにし、顧客がコンテンツ・プロバイダ101によって設定された日付前にその歌曲をダウンロードしてその歌曲を再生する準備ができるようにする。このため、リリース日に帯域幅およびダウンロード時間に対して不満をなくす必要なしに、リリース日にコンテンツ113を直ちにオープンすることができる。

【0160】C. 国別固有パラメータ

任意選択で、クリアリング・ハウス105は、エンドユーザ装置109のドメイン名と、可能であれば、クレジット・カード請求アドレスを使用して、エンドユーザの国別位置を判定する。エンドユーザが在住する国内でコンテンツ113の販売に関する何らかの制限がある場合、クリアリング・ハウス105は、エンドユーザ装置109にライセンスSC660を伝送する前に処理中のトランザクションがこれらの制限のいずれにも違反しないことを保証する。また、電子デジタル・コンテンツ・ストア103も、クリアリング・ハウス105と同じチェックを実行することにより様々な国へのコンテンツ113の配布の管理に関与するものと予想される。クリアリング・ハウス105は、コンテンツ・プロバイダ101が設定した国別固有規則を電子デジタル・コンテンツ・ストア103が無視する場合にそれが行えるものであればどんなチェックでも実行する。

【0161】D. 監査ログおよび追跡

クリアリング・ハウス105は、コンテンツ113の購入トランザクションおよび報告要求トランザクション中に実行される各動作に関する情報の監査ログ150を維持する。この情報は、セキュア・デジタル・コンテンツ電子配布システム100の監査、報告書の作成、データ・マイニングなど、様々な目的に使用することができる。

【0162】また、クリアリング・ハウス105は、電子デジタル・コンテンツ・ストア103用の請求サブシステム182において口座残高も維持する。電子デジタル・コンテンツ・ストア103用の価格設定構造は、デジタル・コンテンツ・レーベルによってクリアリング・ハウス105に提供される。この情報は、電子デジタル・コンテンツ・ストア103に課す必要がある現行特価、ボリューム割引、口座残高不足限度のようなものを含むことができる。クリアリング・ハウス105は価格設定情報を使用して、電子デジタル・コンテンツ・ストア103の残高を追跡し、コンテンツ・プロバイダ101が設定したその残高不足限度を超えないことを保証する。

【0163】以下の動作は、通常、クリアリング・ハウス105によってログ記録される。

・ライセンスSC660を求めるエンドユーザ装置109の要求

- ・ クリアリング・ハウス105が請求を処理する際のクレジット・カード認証番号
- ・ エンドユーザ装置109へのライセンスSC660の分散

- ・ 報告を求める要求
- ・ コンテンツSC630およびライセンスSC660を受け取り、妥当性検査したというエンドユーザからの通知

【0164】以下の情報は、通常、ライセンスSC660に関してクリアリング・ハウス105によってログ記録される。

- ・ 要求の日付と時刻
- ・ 購入トランザクションの日付と時刻
- ・ 購入する項目のコンテンツID
- ・ コンテンツ・プロバイダ101の識別名
- ・ ストア使用条件519
- ・ ウォータマーク命令の変更
- ・ 電子デジタル・コンテンツ・ストア103によって追加されたトランザクションID535
- ・ 電子デジタル・コンテンツ・ストア103の識別名
- ・ エンドユーザ装置109の識別名
- ・ エンドユーザのクレジット・カード情報（クリアリング・ハウス105が請求を処理する場合）

【0165】以下の情報は、通常、エンドユーザのクレジット・カード妥当性検査に関してクリアリング・ハウス105によってログ記録される。

- ・ 要求の日付と時刻
- ・ クレジット・カードに請求される金額
- ・ 購入する項目のコンテンツID
- ・ 電子デジタル・コンテンツ・ストア103によって追加されたトランザクションID535
- ・ 電子デジタル・コンテンツ・ストア103の識別名

- ・ エンドユーザ装置の識別名
- ・ エンドユーザのクレジット・カード情報
- ・ クレジット・カードの決済業者から受け取った認証番号

【0166】以下の情報は、通常、ライセンスSC660がエンドユーザ装置109に送られたときにクリアリング・ハウス105によってログ記録される。

- ・ 要求の日付と時刻
- ・ 購入する項目のコンテンツID
- ・ コンテンツ・プロバイダ101の識別名
- ・ 使用条件517
- ・ 電子デジタル・コンテンツ・ストア103によって追加されたトランザクションID535
- ・ 電子デジタル・コンテンツ・ストア103の識別名
- ・ エンドユーザ装置の識別名

【0167】以下の情報は、通常、報告要求が行われたときにログ記録される。

- ・ 要求の日付と時刻
- ・ 報告が送られた日付と時刻
- ・ 要求された報告のタイプ
- ・ 報告書を作成するために使用するパラメータ
- ・ 報告を要求したエンティティの識別子

【0168】E. 結果の報告

報告書は、クリアリング・ハウス105がエンドユーザの購入トランザクション中にログ記録した情報を使用して、クリアリング・ハウス105によって作成される。コンテンツ・プロバイダ101と電子デジタル・コンテンツ・ストア103は、クリアリング・ハウス105によってログ記録された情報とそれ自身のトランザクション・データベースとの調停を行えるように、支払検証インタフェース183を介してクリアリング・ハウス105からトランザクション報告を要求することができる。また、クリアリング・ハウス105は、コンテンツ・プロバイダ101および電子デジタル・コンテンツ・ストア103に対して定期的な報告を行うこともできる。

【0169】クリアリング・ハウス105は、コンテンツ・プロバイダ101および電子デジタル・コンテンツ・ストア103が報告を要求し受け取れるようにする、安全な電子インタフェースを定義する。報告要求SCは、要求を行ったエンティティにクリアリング・ハウス105が割り当てた証書を含む。クリアリング・ハウス105はその証書とSCのデジタル・シグニチャを使用して、その要求が認可エンティティから出されたことを検証する。また、この要求は、期間など、報告の範囲を定義するパラメータも含む。クリアリング・ハウス105は要求パラメータを妥当性検査し、要求側がそれに関して有することが許された情報だけを受け取れることを保証する。

【0170】報告要求SCが真正かつ有効であるとクリアリング・ハウス105が判断した場合、クリアリング・ハウス105は報告書を作成し、要求を出したエンティティに送るべき報告SCにそれをバックする。報告書によっては、要求を受け取ったときに直ちに送ることができるように、定義された時間間隔で自動的に作成され、クリアリング・ハウス105に記憶される場合もある。報告書に含まれるデータのフォーマットは本書の今後のバージョンで定義される。

【0171】F. 請求および支払検証

コンテンツ113の請求は、クリアリング・ハウス105または電子デジタル・コンテンツ・ストア103のいずれかによって処理することができる。クリアリング・ハウス105が電子コンテンツ113の請求を処理する場合、電子デジタル・コンテンツ・ストア103はエンドユーザのオーダを分離して電子商品にし、適用可

能であれば、物理的商品にする。次に、電子デジタル・コンテンツ・ストア103は、エンドユーザの請求情報を含むトランザクションと、認証する必要がある合計金額についてクリアリング・ハウス105に通知する。クリアリング・ハウス105はエンドユーザのクレジット・カードを認証し、電子デジタル・コンテンツ・ストア103に通知を返す。クリアリング・ハウス105がエンドユーザのクレジット・カードを認証すると同時に、電子デジタル・コンテンツ・ストア103は購入する物理的商品についてエンドユーザのクレジット・カードに請求することができる。エンドユーザ装置109が各電子項目をダウンロードした後、クリアリング・ハウス105は、エンドユーザのクレジット・カードに請求できるように通知を受ける。これは、エンドユーザ装置109での使用のためにコンテンツ113を使用可能にする前に、エンドユーザ装置109による最後のステップとして行われる。

【0172】電子デジタル・コンテンツ・ストア103が電子コンテンツ113の請求を処理する場合、クリアリング・ハウス105は、エンドユーザ装置109がクリアリング・ハウス105にオーダーSC650を送るまでトランザクションに関する通知を受け取らない。クリアリング・ハウス105は、各電子項目をダウンロードした後でエンドユーザ装置109から通知を受ける。クリアリング・ハウス105は、通知を受けると、電子デジタル・コンテンツ・ストア103がエンドユーザのクレジット・カードに請求できるように電子デジタル・コンテンツ・ストア103に通知を送る。

【0173】G. 再伝送

セキュア・デジタル・コンテンツ電子配布システム100は、コンテンツ113の再伝送を処理する能力を提供する。これは、通常、顧客サービス・インタフェース184によって実行される。電子デジタル・コンテンツ・ストア103は、再伝送を開始するためにエンドユーザが段階的に実行できるユーザ・インタフェースを提供する。エンドユーザは、コンテンツ113の再伝送を要求するためにコンテンツ113の項目を購入した電子デジタル・コンテンツ・ストア103のサイトへ移動する。

【0174】コンテンツ113の再伝送は、コンテンツ113がダウンロードできなかったかまたはダウンロードしたコンテンツ113が使用不能であるためにエンドユーザが前に購入したコンテンツ113の項目の新しいコピーを要求したときに行われる。電子デジタル・コンテンツ・ストア103は、コンテンツ113の再伝送を実行する資格がエンドユーザに与えられているかどうかを判定する。再伝送の資格がエンドユーザに与えられている場合、電子デジタル・コンテンツ・ストア103は、再伝送するコンテンツ113の項目のオフターSC641を含むトランザクションSC640を構築す

る。トランザクションSC640はエンドユーザ装置109に送られ、購入トランザクションの場合と同一のステップがエンドユーザによって行われる。エンドユーザ装置109が再伝送されるコンテンツ113の項目用のキー・ライブラリ内にスクランブル済みキーを有する場合、トランザクションSC640は、スクランブル済みキーを削除するようエンドユーザ装置109に指示する情報を含む。

【0175】クリアリング・ハウス105がコンテンツ113の購入の金融決済を処理する場合、電子デジタル・コンテンツ・ストア103は、オーダーSC650でクリアリング・ハウス105に転送されるフラグをトランザクションSC640に含める。クリアリング・ハウス105は、オーダーSC650内のフラグを解釈し、コンテンツ113の購入についてエンドユーザに請求せずにトランザクションを続行する。

【0176】VIII. コンテンツ・プロバイダ

A. 概要

セキュア・デジタル・コンテンツ電子配布システム100におけるコンテンツ・プロバイダ101は、コンテンツ113に対する権利を所有するデジタル・コンテンツ・レーベルまたはエンティティである。コンテンツ・プロバイダ101の役割は、コンテンツ113を配布用に作成し、電子デジタル・コンテンツ・ストア103またはコンテンツ113のダウンロード可能な電子バージョンの小売業者に対しコンテンツ113に関する情報を使用可能にすることである。コンテンツ・プロバイダ101に対し最大限のセキュリティと権利制御を提供するため、コンテンツ113がコンテンツ・プロバイダ101のドメインを去るときにそれが安全であり、無許可当事者によって決して公表されずアクセス不能になるように、コンテンツ・プロバイダがその構内で自分のコンテンツ113を作成してSC内に確実にパッケージ化できるようにするための一連のツールが用意されている。このため、コンテンツ113は、ハッカまたは無許可当事者に対して公表される恐れなしに、インターネットなどの安全ではないネットワークのいたるところに自由に配布することができる。

【0177】コンテンツ・プロバイダ101用のツールの最終的な目標は、1つの歌曲または一連の歌曲などのコンテンツ113を作成してコンテンツSC630内にパッケージ化することと、その歌曲を説明する情報、その歌曲の承認済み用途（コンテンツの使用条件517）、その歌曲に関するプロモーション情報をメタデータSC620内にパッケージ化することである。これを実施するため、以下の1組のツールが用意されている。

・ ワーク・フロー・マネージャ154 - 処理活動をスケジューリングし、プロセス同士の必須の同期を管理する。

・ コンテンツ処理ツール155 - ウォータマー

ク、前処理（オーディオ例の場合、必須の等化、強弱の変化の調節、再サンプリング）、コード化、圧縮を含む、コンテンツ113のファイル作成を制御するためのツールの集合。

・ メタデータ同化入力ツール161 - コンテンツ・プロバイダのデータベース160または第三者のデータベースあるいはデータ・インポート・ファイルからもしくはオペレータの対話によりコンテンツ113の記述情報を収集するために使用するツールの集合であって、コンテンツの使用条件517を指定するための手段を提供する。また、CDまたはDDPファイル用のデジタル・オーディオ・コンテンツなどのコンテンツを取り込むかまたは抽出するためのインタフェースも提供する。

・ 品質管理ツールは、作成したコンテンツおよびメタデータのブリービューを可能にする。メタデータに加える必要がある訂正またはさらに処理するためのコンテンツの再提示を行うことができる。

・ SCバックアップツール152 - すべてのコンテンツ113および情報を暗号化してパッケージ化し、SCバックアップを呼び出してSC内にバックアップする。

・ コンテンツ分散ツール（図示せず） - コンテンツ・ホスト・サイト111および電子デジタル・コンテンツ・ストア103などの指定の配布センターにSCを分散する。

・ コンテンツ・プロモーション・ウェブ・サイト156 - 認可電子デジタル・コンテンツ・ストア103によるダウンロードのためにメタデータSC620および任意選択で追加のプロモーション素材を記憶する。

【0178】B. ワーク・フロー・マネージャ154 このツールの目的は、コンテンツ113の処理活動をスケジューリングし、追跡し、管理することである。このアプリケーションにより、マルチユーザ・アクセスが可能になると同時に、コンテンツ・プロバイダ101のイントラネットまたはエクストラネット内のリモート位置からコンテンツ113のスケジューリングおよび状況チェックが可能になる。また、この設計は協調処理も可能にし、その場合、複数の個人がコンテンツ113の複数のピースについて並行して作業することができ、それぞれ異なる個人に特定の責任を割り当てることができ、このような個人を世界中に分散させることができる。

【0179】次に図11に移行すると、図10に対応するワーク・フロー・マネージャ154の主要プロセスを示すブロック図である。図11の主要プロセスは、この項で説明するツールによって提供されるコンテンツ113処理機能を要約したものである。ワーク・フロー・マネージャ154は、これらのプロセスにジョブを供給し、その現行プロセスの完了時に次の必須プロセスにジョブを向けることを担当する。これは、以下の動作を実行するために各処理ツールが呼び出す一連のアプリケーション・プログラミング・インタフェース（API）に

より実施される。

- ・ 処理すべき次のジョブを取り出す。
- ・ プロセスの正常終了を示す。
- ・ プロセスの終了失敗とその失敗の理由を示す。
- ・ プロセスの暫定状況を示す（従属プロセスの部分完了のみを必要とするプロセスの開始を可能にするため）
- ・ 指定のプロセスにとって使用可能なコメントを製品に追加する。

【0180】ワーク・フロー・マネージャ154はユーザ・インタフェースも有し、一例としてワーク・フロー・マネージャ・ユーザ・インタフェース700を図10に示すが、これは以下の機能を提供する。

- ・ 処理の様々な段階で割り当てて実行すべきデフォルト値および条件の指定を可能にするための構成パネル
- ・ ワーク・フロー規則および自動処理フローのカスタマイズ

・ ジョブ・スケジューリング

・ 状況照会および報告

・ 1つまたは複数のプロセスに関連するジョブのコメントまたは命令を追加すること

・ ジョブ管理（すなわち、中断、解放、除去、優先順位（処理の順序）変更）

【0181】各プロセスは、それに関連する待ち行列をワーク・フロー・マネージャ154によって管理させる。いずれのプロセスもワーク・フロー・マネージャ154からジョブを要求すると、その結果、ワーク・フロー・マネージャ154は、その関連待ち行列内に現在いかなるジョブも存在しない場合にプロセス（ツール）を中断して待ち状態にするか、それぞれのプロセスを実行するために必要なジョブに関するすべての情報をプロセスに返す。プロセスを中断して待ち状態にした場合、ワーク・フロー・マネージャ154によってその待ち行列にジョブが置かれると、そのプロセスが処理を再開する。

【0182】また、ワーク・フロー・マネージャ154は、1組の定義済み規則に基づいて処理のフローまたは順序も管理する。これらの規則は、コンテンツ・プロバイダ101が特殊処理要件を有するかまたは特定のデフォルト規則を構成する場合に、そのプロバイダによってカスタマイズすることができる。あるプロセスがその割当てタスクの完了を報告すると、そのプロセスはワーク・フロー・マネージャ154にこの状況を通知し、ワーク・フロー・マネージャ154は定義済み規則に基づいて次にそのジョブがどの待ち行列に置かれるかを決定する。

【0183】プログラミングAPIによるかまたはワーク・フロー・マネージャ・ユーザ・インタフェース700またはプロセッサ・インタフェースにより手動で、いずれかの処理ステップで特殊処理命令または通知を示すコメントも製品に付加することができる。

【0184】ワーク・フロー・マネージャ154におけるプロセスは、好ましい実施形態ではJavaで実現されるが、C/C++、アセンブラ、それと同等のものなどのその他のプログラミング言語も使用することができる。ただし、ワーク・フロー・マネージャ154に関して後述するプロセスは様々なハードウェアおよびソフトウェア・プラットフォーム上で実行できることに留意されたい。完全なシステムとしてまたはその構成プロセスのいずれかとしてのワーク・フロー・マネージャ154は、ウェブなどの電子配布またはフロッピー（登録商標）・ディスク、CD-ROM、取外し可能ハード・ディスク・ドライブを含みかつこれに限定されないコンピュータ可読媒体に入れてアプリケーション・プログラムとして配布することができる。

【0185】次に図11に移行すると、図10に対応するワーク・フロー・マネージャ154の主要プロセスを示すブロック図である。以下の各項では、各プロセスについて要約し、各プロセスが必要とする情報またはアクションについて説明する。

【0186】1. 製品待受けアクション／情報プロセス 801

そのプロセスが必要とするすべての情報が使用可能になり、そのジョブがすべての従属処理をすでに正常に完了していると、特定のプロセス待ち行列にジョブが置かれる。ワーク・フロー・マネージャ154には、情報の欠落またはその後の処理を妨げるような障害のために、現在、処理に使用可能ではないジョブを保持するために使用する特殊待ち行列が存在する。これらのジョブは、製品待受けアクション／情報プロセス801の待ち行列に置かれる。この待ち行列内の各ジョブは、それが対応するアクションまたは情報、このジョブに作用した最後のプロセス、欠落情報または追加の情報が提供されるかまたは必須アクションが正常に完了したときにこのジョブが待ち行列化される次のプロセスを示すために関連状況を有する。

【0187】いずれかのプロセスが完了すると、ワーク・フロー・マネージャ154はこの待ち行列をチェックし、この待ち行列内のいずれかのジョブがこのプロセス（アクション）の完了またはこのプロセスによって提供される情報を待っているかどうかを判定する。そうである場合、そのジョブは適切なプロセス待ち行列に待ち行列化される。

【0188】2. 新コンテンツ要求プロセス802

コンテンツ・プロバイダ101は、それが販売し、電子的に送達したいと希望する製品（たとえば、製品は1曲の歌曲である場合もあれば、複数歌曲の集合である場合もある）を決定する。ワーク・フロー・マネージャ154の初期機能は、オペレータがこのような製品を識別し、それを新コンテンツ要求プロセス802の待ち行列に置くことができるようにすることである。コンテンツ

・プロバイダ101は、製品選択インタフェースでどの情報が要求されるかを構成オプションにより指定することができる。その製品を明確に識別するために十分な情報が入力される。任意選択で、メタデータ収集と並行してオーディオ処理フェーズを開始するために必要な情報の手動入力を要求するために、追加のフィールドを含めることもできる。手動で提供されない場合、任意選択で、自動メタデータ収集プロセス803のようにメタデータ処理の第1の段階で得られるコンテンツ・プロバイダのデータベース160からまたはデフォルト構成設定からこの情報を取り出すことができる。コンテンツ・プロバイダのデータベース160におけるコンテンツ113の構成および諸機能によってコンテンツ選択プロセスが決定される。

【0189】コンテンツ・プロバイダ101のデータベース160への照会を実行するために必要な必須情報が指定された場合、そのジョブは自動メタデータ収集プロセス803によって処理される。音楽の実施形態では、オーディオ処理のためにその製品を適切にスケジューリングするために、製品のジャンルと所望の圧縮レベルならびにオーディオPCMまたはWAVファイル名が指定される。この情報は、製品選択プロセスの一部として入力するかまたはカスタマイズ照会インタフェースまたはウェブ・ブラウザ機能により選択することができる。この情報を指定すると、コンテンツ処理のために製品をスケジューリングすることができる。

【0190】製品選択ユーザ・インタフェースは、処理のために製品をリリースできるかどうかまたは追加の情報入力までそれを保持するかどうかをオペレータが指定できるようにするオプションを提供する。保持する場合、ジョブは新コンテンツ要求プロセス802の待ち行列に追加され、データ入力を完了するかまたは処理のためにその製品をリリースするかあるいはその両方のために次のアクションを待つ。製品がリリースされると、ワーク・フロー・マネージャ154は指定した情報を評価し、どのプロセスがそのジョブに渡される状態になっているかを判定する。

【0191】コンテンツ・プロバイダ101のデータベース160に対する自動照会を可能にするために十分な情報が提供された場合、そのジョブは自動メタデータ収集プロセス803のために待ち行列化される。自動メタデータ収集プロセス803のためにデータベース・マッピング・テーブルが構成されていない場合、そのジョブは手動メタデータ入力プロセス804のために待ち行列化される（データベース・マッピング・テーブルに関する詳細については自動メタデータ収集プロセス803の項を参照）。

【0192】オーディオ処理のための必須一般情報とウォーターマークに必要な特殊情報が指定された場合、そのジョブはウォーターマーク・プロセス808（コンテンツ

処理の第1のフェーズ)のために待ち行列化される。ジョブがリリースされたときに必須情報のいずれかが欠落している場合、そのジョブは、欠落した情報を示す状況とともに、製品待受けアクション/情報プロセス801の待ち行列に待ち行列化される。

【0193】たとえば、コンテンツ113がオーディオであり、PCMまたはWAVファイルが欠落しているようなコンテンツ113のファイル名をその状況が示す場合、これは、取込み(またはデジタル媒体からのデジタル抽出)が必要であることを示す場合もある。オーディオ処理機能では、歌曲ファイルは標準のファイル・システム・インタフェースによりアクセス可能でなければならない。歌曲が外部媒体またはオーディオ処理ツールが直接アクセスできないファイル・システム上に位置する場合、そのファイルはまずアクセス可能なファイル・システムにコピーされる。歌曲がデジタル・フォーマットになっているがCDまたはデジタル・テープ上にある場合、その歌曲はオーディオ処理ツールにとってアクセス可能なファイル・システムに抽出される。そのファイルがアクセス可能になると、ウォータマークに必要な他のすべての情報もすでに指定されていると想定し、ワーク・フロー・マネージャ・ユーザ・インタフェース700を使用して、それをウォータマーク・プロセスにリリースできるようにそのジョブ用のパスおよびファイル名を指定または選択する。

【0194】3. 自動メタデータ収集プロセス803
自動メタデータ収集プロセス803は、製品情報のうちのできるだけ多くを自動的に入手しようと試みて、コンテンツ・プロバイダ101のデータベース160またはデータがインポートされたステージング・データベースへの一連の照会を実行する。自動メタデータ収集プロセス803では、その待ち行列に項目を置けるようになる前に以下の情報を必要とする。コンテンツ・プロバイダ101のデータベース160への照会を生成するために十分な情報を備えたデータベース・マッピング・テーブル

- ・ 照会を実行するために必要な製品情報
- ・ 製品を明確に定義するために十分な製品情報

【0195】このコンテンツ113を処理するために必要な情報を入手するために、コンテンツ・プロバイダ101のデータベース160への自動照会が実行される。たとえば、コンテンツ113が音楽である場合、この照会を実行するために必要な情報はアルバム名にすることもできるが、UPCであるかまたはコンテンツ・プロバイダ101によって定義された特定のアルバムまたは選択IDにすることもできる。入手すべき情報の一部は必須のものとして指定される(詳細については自動メタデータ収集プロセス803に関する項を参照)。すべての必須情報を入手した場合、次にそのジョブは使用条件プロセス805のために待ち行列化される。いずれかの必

須情報が欠落している場合、その歌曲は手動メタデータ入力プロセス804のために待ち行列化される。製品待受けアクション/情報プロセス801の待ち行列内のいずれかのジョブがこのステップで入手した情報のいずれかを待っている場合、それがもはやこの情報を待っていないことを示すためにジョブ状況が更新される。そのジョブがもはや未処理の要件を持っていない場合、それは次の定義済み待ち行列に待ち行列化される。

【0196】4. 手動メタデータ入力プロセス804

10 手動メタデータ入力プロセス804は、オペレータが欠落情報を入力するための手段を提供する。これには、依存関係はない。すべての必須情報が指定されると、そのジョブは使用条件プロセス805のために待ち行列化される。

【0197】5. 使用条件プロセス805

使用条件プロセス805は、製品用途および制限の指定を可能にするものである。使用条件プロセス805は何らかのメタデータを必要とする場合がある。使用条件の指定が完了すると、そのジョブは、監視付きリリース・プロセス806オブションがすでに要求されたかまたはワーク・フロー・マネージャ154の規則にデフォルトとして構成されるまで、メタデータSC作成プロセス807のために待ち行列化される資格が与えられる。その場合、そのジョブは監視付きリリース・プロセス806のために待ち行列化される。メタデータSC作成プロセス807に待ち行列化する前に、ワーク・フロー・マネージャ154はまず、そのプロセスに関するすべての依存関係が満たされていることを保証する(以下参照)。そうではない場合、そのジョブは製品待受けアクション/情報プロセス801に待ち行列化される。

【0198】6. 監視付きリリース・プロセス806

監視付きリリース・プロセス806は、デジタル・コンテンツ製品について指定された情報の品質チェックおよび妥当性検査を可能にする。これには、いかなる依存関係もない。この製品の処理のいずれかの段階でそのジョブに事前に付加したコメントはスーパーバイザが検討し、適切なアクションを講じることができる。すべての情報およびコメントの検討後、スーパーバイザは以下のオブションを有する。

・ リリースを承認し、メタデータSC作成プロセス807のためにその製品を待ち行列化する。

・ 情報の変更または追加あるいはその両方を行い、メタデータSC作成プロセス807のためにその製品を待ち行列化する。

・ そのジョブにコメントを追加し、手動メタデータ入力プロセス804のために再待ち行列化する。

・ コメントを追加し、製品待受けアクション/情報プロセス801のための待ち行列にそのジョブを待ち行列化する。

【0199】7. メタデータSC作成プロセス807

メタデータSC作成プロセス807は、上記で収集したすべての情報ならびにメタデータSC620に必要なその他の情報をまとめて収集し、SCバック・プロセスを呼び出してメタデータSC620を作成する。このツールは入力として以下のものを必要とする。

- ・ 必須メタデータ
- ・ 使用条件
- ・ この製品のためにすべての品質レベルの暗号化段階で使用する暗号化キー

【0200】この最後の依存関係では、メタデータSC620を作成する前に関連オーディオ・オブジェクトがオーディオ処理フェーズを完了していなければならない。メタデータSC作成プロセス807が完了すると、そのジョブは、定義済みワーク・フロー規則に基づいて最終品質保証プロセス813またはコンテンツ分散プロセス814のいずれかのための待ち行列に待ち行列化される。

【0201】8. ウォータマーク・プロセス808
ウォータマーク・プロセス808は、著作権およびその他の情報をコンテンツ113に追加するものである。コンテンツ113が歌曲である実施形態の場合、このツールは入力として以下のものを必要とする。

- ・ 歌曲ファイル名（アルバムの場合は複数のファイル名）
- ・ ウォータマーク命令
- ・ ウォータマーク・パラメータ（ウォータマークに含める情報）

【0202】ウォータマーク・プロセス808が完了すると、そのジョブは、その必須入力を使用可能である場合には前処理圧縮プロセス809のために待ち行列化され、そうではない場合には製品待受けアクション／情報プロセス801に待ち行列化される。

【0203】9. 前処理圧縮プロセス809
前処理圧縮プロセス809は、指定の圧縮レベルに応じてコンテンツ113をコード化し、どの必須前処理も先に実行する。この待ち行列に1つのジョブを待ち行列化すると、実際には、複数の待ち行列項目が作成される。所望の製品の各圧縮レベルごとに1つのジョブが作成される。コード化プロセスは、複数のシステムで並行して実行することができる。このツールは以下の入力が必要とする。

- ・ ウォータマーク付きコンテンツ・ファイル名（コンテンツ113がアルバムの場合は複数のファイル名）
- ・ 製品の品質レベル（事前構成可能）
- ・ 圧縮アルゴリズム（事前構成可能）
- ・ 製品ジャンル（プリプロセッサが必要とする場合）

【0204】コード化プロセスが完了すると、そのジョブは、ワーク・フロー規則によって構成された場合にはコンテンツ品質管理プロセス810に待ち行列化される。そうではない場合には、ジョブは暗号化プロセス8

11のために待ち行列化される。

【0205】オーディオなどのコンテンツ113のうち、すでに処理されたコンテンツの割合を表示するための方法またはコンテンツ113のうち、すでにコード化されたコンテンツの量を選択したコンテンツ113の選択内容全体のうちの割合として示すための方法をコード化ツールの第三者プロバイダが提供しない場合、図11のコンテンツ前処理圧縮ツール用のデジタル・コンテンツのコード化速度を決定するための方法の流れ図1100を図14に示す。この方法は、ステップ1101における所望のコード化アルゴリズムおよびビット伝送速度の選択から始まる。次に、ステップ1102では、このアルゴリズムおよびコード化速度が前に計算された速度係数を有するかどうかを判定するための照会を行う。この速度係数は、特定のコード化アルゴリズムおよび特定のビット伝送速度の場合の圧縮速度を決定するために使用する係数である。前に計算された速度係数が一切記憶されていない場合、所定量の時間の間、コンテンツ113のサンプルをコード化する。好ましい実施形態では、所定の期間は数秒である。所定の期間用のこのコード化速度を使用して、新しい速度係数 R_{NEW} を計算する。ステップ1108では、時間の量およびコード化したコンテンツ113の量を把握して、 $R_{NEW} = (\text{コード化したデジタル・コンテンツの長さ}) / (\text{時間の量})$ として新しい速度係数 R_{NEW} を計算する。ステップ1109では、コンテンツ113をコード化し、前に計算された速度係数 R_{NEW} を使用してコード化状況を表示する。次に、将来、このコード化アルゴリズムおよびコード化ビット伝送速度に使用するために、ステップ1107でこのコード化速度係数 R_{NEW} を記憶する。ステップ1103で選択したアルゴリズムが前に計算された速度係数 R_{STORED} を有する場合、ステップ1104でコンテンツ113をコード化し、前に計算された速度係数 R_{STORED} を使用して経過を表示する。その間に、ステップ1105でこの選択したアルゴリズムおよびビット伝送速度について、現行速度係数 $R_{CURRENT}$ を計算する。ステップ1106では、この現行速度係数 $R_{CURRENT}$ を使用して、記憶した速度係数を $R_{NEW} = (R_{STORED} + R_{CURRENT})$ の平均として更新する。速度係数の反復更新により、その後、特定のコード化アルゴリズムおよびビット伝送速度に使用するたびに、コード化速度の決定がますます正確なものになりうる。ステップ1107では、今後の使用のために新しい速度 R_{NEW} を記憶する。現行速度係数 $R_{CURRENT}$ が所与の範囲またはしきい値分だけ前に記憶された速度係数 R_{STORED} の範囲を超える場合、 R_{STORED} の更新を行わなくてもよい。

【0206】次に、コード化状況の表示を提示することができる。コード化状況は、現行コード化速度とともに、コード化速度およびコンテンツ113用のファイルの全長に基づいて経過バーとして表示される全コンテン

ツ113の割合の表示を含む。また、コード化状況は、コード化のための残り時間も含むことができる。コード化のための残り時間は、計算されたコード化速度RCURRENTをコンテンツ113用のファイルの全長で割ることによって計算することができる。コード化状況は、呼出しプロセスを呼び出すことができる他のプログラムに転送することができる。このことによって、コード化に対する監視プログラムまたはコード化時の共依存プログラムが操作され、かつ、より効率よく処理するためにバッチ処理されることを促進できる。ただし、代替実施形態では、コード化がウォーターマーク付けのステップを含む可能性があることに留意されたい。

【0207】10. コンテンツ品質管理プロセス810
コンテンツ品質管理プロセス810は、機能の点で監視付きリリース・プロセス806と同様のものである。これは、誰かがこれまでに実行されたコンテンツ処理の品質を妥当性検査できるようにする任意選択ステップである。これは、ウォーターマーク・プロセス808の完了および前処理圧縮プロセス809のコード化部分以外にいかなる依存関係も持っていない。コンテンツ品質管理プロセス810が完了すると、以下のオプションが使用可能になる。

- ・ そのジョブをリリースし、暗号化プロセス811のために待ち行列化することができる。

- ・ コメントを付加し、1つまたは複数のジョブを前処理圧縮プロセス809のために再待ち行列化することができる。

【0208】最後のオプションでは、コンテンツ品質管理プロセス810の後まで歌曲ファイルの未コード化ウォーターマーク付きバージョンが引き続き使用可能でなければならない。

【0209】11. 暗号化プロセス811

暗号化プロセス811は、適切なセキュア・デジタル・コンテンツ電子配布権利管理機能と呼び出して、ウォーターマーク付き／コード化歌曲ファイルのそれぞれを暗号化する。このプロセスは、他のすべてのオーディオ処理の完了以外にいかなる依存関係も持っていない。暗号化プロセス811のプロセスが完了すると、そのジョブはコンテンツSC作成プロセス812のために待ち行列化される。

【0210】12. コンテンツSC作成プロセス812
コンテンツSC作成プロセス812のプロセスでは、何らかのメタデータ・ファイルをコンテンツSC630に含めなければならない場合がある。コンテンツ113以外のファイルが必要な場合、そのファイルを収集し、SCバックアップ・プロセスを呼び出して、作成したコンテンツ113（たとえば、歌曲）の各圧縮レベルごとにコンテンツSC630を作成する。コンテンツSC作成プロセス812が完了すると、その歌曲は、定義済みワーク・フロー規則に基づいて最終品質保証プロセス813また

はコンテンツ分散プロセス814のいずれかに待ち行列化される。

【0211】13. 最終品質保証プロセス813

最終品質保証プロセス813は、関連メタデータとコンテンツSC630との相互参照チェックにより、両者が正しく一致し、そこに含まれるすべての情報およびコンテンツ113が正しいものであることを検証できるようにする任意選択ステップである。最終品質保証プロセス813が完了すると、そのジョブはコンテンツ分散プロセス814のために待ち行列化される。問題が見つかった場合、ほとんどの場合、そのジョブは失敗した段階に再待ち行列化しなければならない。製品は、問題を訂正するために必要な再処理に加え、再暗号化および再バックを経なければならないので、この段階での手直しは非常に高価なものになる。従来の保証段階を使用して、コンテンツ113の品質および情報の正確さと完璧さを保証することを大いに推奨する。

【0212】14. コンテンツ分散プロセス814

コンテンツ分散プロセス814のプロセスは、適切なホスト・サイトへのSCの転送を担当する。SCの正常転送後、ジョブ完了状況がログ記録され、そのジョブが待ち行列から削除される。SCの転送時に問題が発生した場合、定義した回数の試行後に、そのジョブは、ワーク・フロー・マネージャ・ツール154において、検出されたエラーとともに、失敗したことを示すフラグが付けられる。

【0213】15. ワーク・フロー規則

図11に関するワーク・フロー規則は、以下のように3つの主要システムで機能する。

A: ワーク・フロー・マネージャ・ツール154

1. 新コンテンツ要求プロセス802
2. 製品待受けアクション／情報プロセス801
3. 最終品質保証プロセス813
4. コンテンツ分散（および通知）プロセス814

B: メタデータ同化入力ツール161

1. 自動メタデータ収集プロセス803
2. 手動メタデータ入力プロセス804
3. 監視付きリリース・プロセス806
4. メタデータSC作成プロセス807

C: コンテンツ処理ツール155

1. ウォーターマーク・プロセス808（著作権データを必要とする）
2. 前処理圧縮プロセス809
3. コンテンツ品質管理プロセス810
4. 暗号化ツール811
5. コンテンツSC作成プロセス812

【0214】ワーク・フロー

コンテンツ113選択オペレータは新しい製品を入力し、A1（新コンテンツ要求プロセス802）への待ち行列化に取りかかる。

A1: コンテンツ113選択オペレータがそれをワーク・フロー・マネージャ・ツール154にリリースすると、それはB1(自動メタデータ収集プロセス803)に待ち行列化される

A2: ステップB1(自動メタデータ収集プロセス803)からまたはステップB2(手動メタデータ入力プロセス804)からまたはステップB3(監視付きリリース・プロセス806)から先行ステップ(メタデータSC作成プロセス807)への途上[暗号化キーを必要とする]先行ステップ(メタデータSC作成プロセス807)からステップA3(最終品質保証プロセス813)またはステップA4(コンテンツ分散プロセス814)への途上[コンテンツSC630を必要とする]ステップC1(ウォーターマーク・プロセス808)からステップC2(前処理圧縮プロセス809)への途上[前処理圧縮プロセス809用のメタデータを必要とする]ステップC4(暗号化プロセス811)からステップC5(コンテンツSC作成プロセス812)への途上[コンテンツSC630バッキング用のメタデータを必要とする]ステップC5(コンテンツSC作成プロセス812)からステップA3(最終品質保証プロセス813)またはステップA4(コンテンツ分散プロセス814)への途上[メタデータSC620を必要とする]

A3: ステップA3(最終品質保証プロセス813)後に待ち行列B2(手動メタデータ入力プロセス804)上に置くかまたは待ち行列B3(監視付きリリース・プロセス806)上に置くかまたは品質保証オペレータが要求する待ち行列内に入れる

A4: ステップA4(コンテンツ分散プロセス814)後にこの製品についてワーク・フロー・マネージャ・ツール154が実行される

B1: ステップB1(自動メタデータ収集プロセス803)後にステップC1(ウォーターマーク・プロセス808)に必要なメタデータが存在する場合、この製品を表す項目を待ち行列C1上に置く(以下の論理も実行する)1-いずれかの必須メタデータが欠落しているかまたは2-手動メタデータ・プロバイダに向けられたコメントが存在する場合、その製品を待ち行列B2(手動メタデータ入力プロセス804)上にも置くあるいはこの製品について監視付きリリースが要求された場合、その製品を待ち行列B3(監視付きリリース・プロセス806)上に置くあるいはその製品が要求されたすべての品質レベルについてコンテンツ処理ツール155からのすべての情報を有する場合、その製品を先行待ち行列(メタデータSC作成プロセス807)上に置くあるいは暗号化キーを必要とすることを示すフラグをその製品に付け、その製品を待ち行列A2(製品待受けアクション/情報プロセス801)上に置く

B2: ステップB2(手動メタデータ入力プロセス804)中にステップC1(ウォーターマーク・プロセス80

8)が実行されておらず、しかもステップC1に必要なメタデータが存在する場合、この製品を表す項目を待ち行列C1上に置く(以下の論理も実行する)ステップC2(前処理圧縮プロセス809)に必要なメタデータが提供されたばかりである場合(以下の論理も実行する)メタデータ同化入力ツール161が収集可能なメタデータが存在する場合この製品について監視付きリリースが要求された場合、その製品を待ち行列B3(監視付きリリース・プロセス806)上に置くあるいはコンテンツ処理ツール155のステップC4(暗号化プロセス811)からのすべての情報が存在する場合、この製品を先行待ち行列(メタデータSC作成プロセス807)上に置くあるいは暗号化キーを必要とすることを示すフラグをその製品に付け、この製品を待ち行列A2(製品待受けアクション/情報プロセス801)上に置くあるいはメタデータ・プロバイダが強制監視付きリリースを要求した場合、その製品を待ち行列B3(監視付きリリース・プロセス806)上に置くあるいは何も実行しない(その製品を待ち行列B2(手動メタデータ入力プロセス804)上に保持する)

B3: ステップB3(監視付きリリース・プロセス806)中にこのオペレータがステップB2(手動メタデータ入力プロセス804)にその製品を返送する場合、その製品を待ち行列B2上に置くあるいはこのオペレータがその製品をリリースした場合コンテンツ処理ツール155のステップC4(暗号化プロセス811)からのすべての情報が存在する場合、この製品を先行待ち行列(メタデータSC作成プロセス807)上に置くあるいは暗号化キーを必要とすることを示すフラグをその製品に付け、この製品を待ち行列A2(製品待受けアクション/情報プロセス801)上に置くあるいはその製品は待ち行列B2(監視付きリリース・プロセス806)上に存続する

先行: 先行ステップ(メタデータSC作成プロセス807)後にメタデータがバックされたことを示すフラグをその製品に付けるすべての(製品/品質レベル)タブルがバックされた場合コンテンツ・プロバイダ101の構成がSCの品質保証を指定する場合、この製品を待ち行列A3(最終品質保証プロセス813)上に置くあるいはこの製品を待ち行列A4(コンテンツ分散プロセス814)上に置くあるいはコンテンツ113のSCを必要とすることを示すフラグをその製品に付け、この製品を待ち行列A2(製品待受けアクション/情報プロセス801)上に置く

C1: ステップC1(ウォーターマーク・プロセス808)後にステップC2(前処理圧縮プロセス809)に必要なメタデータが存在する場合、各(製品/品質レベル)タブルごとに項目を作成し、それを待ち行列C2上に置くあるいは前処理/圧縮用のメタデータを必要とすることを示すフラグをその製品に付け、この製品を待ち

行列A2（製品待受けアクション／情報プロセス801）上に置く

C2：ステップC2（前処理圧縮プロセス809）後にコンテンツ・プロバイダ101の構成がコンテンツ品質管理プロセス810を指定する場合、この（製品／品質レベル）タブを待ち行列C3（コンテンツ品質管理プロセス810）上に置くあるいはこの（製品／品質レベル）タブを待ち行列C4（暗号化プロセス811）上に置く

C3：ステップC3（コンテンツ品質管理プロセス810）後に、この（製品／品質レベル）タブを待ち行列C4（暗号化プロセス811）上に置く

C4：ステップC4（暗号化プロセス811）後に必要な情報（すなわち、そのプロセスによって生成され、コンテンツ113を暗号化するために使用する対称キー623）をメタデータ同化入力ツール161に供給するコンテンツSC630に必要なすべてのメタデータが存在する場合、この（製品／品質レベル）タブを待ち行列C5（コンテンツSC作成プロセス812）上に置くあるいはコンテンツSC630のバッキングのためにメタデータを必要とすることを示すフラグをその製品に付け、この（製品／品質レベル）タブをA2（製品待受けアクション／情報プロセス801）上に置く

C5：ステップC5（コンテンツSC作成プロセス812）後にこの品質レベルのコンテンツ113がバックされたことを示すフラグをその品質レベルに付けるすべての（製品／品質レベル）タブがバックされた場合メタデータがバックされたことを示すフラグがその製品に付けられた場合コンテンツ・プロバイダ101の構成がSCの品質保証を指定する場合、この製品を待ち行列A3（最終品質保証プロセス813）上に置くあるいはこの製品を待ち行列A4（コンテンツ分散プロセス814）上に置くあるいはメタデータSC620を必要とすることを示すフラグをその製品に付け、この製品を待ち行列A2（製品待受けアクション／情報プロセス801）上に置くあるいは（すべての（製品／品質レベル）タブがバックされていない）何も実行しない（他の（製品／品質レベル）タブがアクションを起動する

【0215】C. メタデータ同化入力ツール

メタデータはコンテンツ113を記述するデータからなり、たとえば音楽では録音のタイトル、アーティスト、著者／作曲家、プロデューサ、録音の長さからなる。以下の説明はコンテンツ113が音楽である場合に基づくものであるが、当業者であれば、その他のコンテンツ・タイプ、たとえば、ビデオ、プログラム、マルチメディア、映画、およびそれと同等のものが本発明の真の範囲および意味に含まれることに留意されたい。

【0216】このサブシステムは、製品の販売のプロモーションを支援するためにコンテンツ・プロバイダ101が電子デジタル・コンテンツ・ストア103に提供

するデータ（たとえば、音楽の場合、このアーティストによるサンプル・クリップ、このアーティストの経歴、この録音が収録されたアルバムのリスト、このアーティストまたは製品あるいはその両方に関連するジャンル）、購入した製品とともにコンテンツ・プロバイダ101がエンドユーザに提供するデータ（たとえば、アーティスト、プロデューサ、アルバム・カバー、トラック長）、コンテンツ・プロバイダ101がエンドユーザに提供したいと希望する各種購入オプション（使用条件517）をひとまとめにものである。このデータはメタデータSC620にパッケージ化され、電子デジタル・コンテンツ・ストア103が使用可能なものになる。これを実施するため、以下のツールが用意されている。

- ・ 自動メタデータ収集ツール
- ・ 手動メタデータ入力ツール
- ・ 使用条件ツール
- ・ 監視付きリリース・ツール

【0217】これらのツールは、コンテンツ・プロバイダ101がワーク・フロー・マネージャ154に関して前述したプロセスを実施できるようにするものである。ここに記載するツールは、好ましい実施形態ではJavaに基づくツールキットであるが、C/C++、アセンブラ、およびそれと同等のものなど、その他のプログラミング言語も使用することができる。

【0218】1. 自動メタデータ収集ツール

自動メタデータ収集ツールは、前述の自動メタデータ収集プロセス803を実施する能力をユーザに提供する。自動メタデータ収集ツールは、コンテンツ・プロバイダ101のデータベース160にアクセスし、オペレータの支援なしにできるだけ多くのデータを取り出すために使用する。このプロセスを自動化するために、構成方法が使用可能である。コンテンツ・プロバイダ101は、このコンテンツ・プロバイダ101がエンドユーザに提供したいと希望するデータのタイプ（たとえば、作曲家、プロデューサ、伴奏楽器奏者、トラック長）およびコンテンツ・プロバイダ101が電子デジタル・コンテンツ・ストア103に提供するプロモーション・データのタイプ（たとえば、音楽の例の場合、このアーティストによるサンプル・クリップ、このアーティストの経歴、この録音が収録されたアルバムのリスト、このアーティストに関連するジャンル）を識別するためにデフォルト・メタデータ・テンプレートを調整することができる。デフォルト・メタデータ・テンプレートとしては、エンドユーザ装置109が必要とするデータ・フィールド、任意選択でエンドユーザ装置109に提供可能なデータ・フィールド、電子デジタル・コンテンツ・ストア103を目標とし、アーティスト、アルバム、またはシングル、あるいはそれらの組合せをプロモーションする複数データ・フィールドからなるサンプル・セットを含む。

【0219】コンテンツ・プロバイダ101のデータベ

ース160からテンプレート・データ・フィールドを抽出するために、自動メタデータ収集ツールは、データのタイプ（たとえば、作曲家、プロデューサ、アーティストの経歴）をデータを検出可能なデータベース内の位置にマッピングするテーブルを使用する。各コンテンツ・プロバイダ101は、それぞれの環境用にマッピング・テーブルを指定するのを支援する。

【0220】自動メタデータ収集ツールは、コンテンツ・プロバイダ101のメタデータ・テンプレートとマッピング・テーブルを使用して、コンテンツ・プロバイダ101のデータベース160から入手可能なものであればどのようなデータでも収集する。各製品の状況は自動メタデータ収集プロセス803の結果によって更新される。何らかの必須データが欠落している製品は手動メタデータ入力プロセス804のために待ち行列化され、そうでない場合、その製品はメタデータSC620にバックするために使用可能である。

【0221】2. 手動メタデータ入力ツール

手動メタデータ入力ツールは、前述の手動メタデータ入力プロセス804を実施する能力をユーザに提供する。手動メタデータ入力ツールは、適切に許可されたオペレータが欠落データを提供できるようにするものである。欠落データが使用不能であるとオペレータが判断した場合、そのオペレータは製品にコメントを付加し、監視付きリリースを要求することができる。コンテンツ・プロバイダ101は、品質保証のために、その製品に対して監視付きリリースを行うことを要求することができる。すべての必須データが存在し、しかも監視付きリリースがまだ要求されていない場合、その製品はメタデータSC620にバックするために使用可能である。

【0222】3. 使用条件ツール

使用条件ツールは、前述の使用条件プロセス805を実施する能力をユーザに提供する。電子送達を使用して販売または貸貸借（限定使用）のためにコンテンツ113を提供するプロセスは一連のビジネス判断を必要とする。コンテンツ・プロバイダ101は、コンテンツ113を使用可能にする圧縮レベルを決定する。次に、コンテンツ113の各圧縮コード化バージョンごとに、1つまたは複数の使用条件を指定する。各使用条件は、コンテンツ113の使用に関してエンドユーザの権利とエンドユーザに対する制限を定義する。

【0223】コンテンツ処理ツール155の一部として、1組の使用条件（エンドユーザの権利および制限）が製品に付加される。

【0224】1つの使用条件は以下のものを定義する。

1. この使用条件が適用されるコンテンツ113の圧縮コード化バージョン
2. この使用条件が適用されるユーザのタイプ（たとえば、企業、個人消費者）
3. この使用条件がコンテンツ113の購入を可能にするか貸貸借を可能にするか
貸貸借トランザクションの場合：
 - ・ 貸貸借の期間を限定するために使用する測定単位（たとえば、日数、再生回数）
 - ・ それ以降コンテンツ113がもはや再生されなくなる上記の単位数購入トランザクションの場合：
 - ・ エンドユーザが作成を許される再生可能コピーの数
 - ・ コピーを作成可能な媒体の種類（たとえば、CDレコーダブル（CD-R）、ミニディスク、パーソナル・コンピュータ）
4. 購入／貸貸借トランザクションを行える期間（すなわち、エンドユーザは、使用可能開始日後であっても使用可能最終日前に限り、この使用条件の条件下で購入／貸貸借を行うことができる）
5. エンドユーザがこの購入（または貸貸借）のトランザクションを行うことができる国
6. この使用条件下での購入／貸貸借トランザクションの価格
7. ウォータマーク・パラメータ
8. クリアリング・ハウス105の通知を必要とするイベントのタイプ

【0225】使用条件のセットの例

コンテンツ・プロバイダ101は、1997年の第4四半期中に人気のある子供向け歌手による子供向け歌曲の再リリースを北米市場が受け入れるかどうかをテストすることを決定する場合がある。このテストでは、この歌曲を384Kbpsと56Kbpsという2通りの圧縮コード化バージョンで提供する。384Kbpsバージョンは購入（およびミニディスク上に1回コピー可能）または貸貸借（2週間）可能であり、56Kbpsバージョンは購入のみ（コピー作成は不可）可能である。ウォータマーク命令はいかなる購入／貸貸借荷についても同じであり、コンテンツ・プロバイダ101は作成したすべてのコピーをクリアリング・ハウス105がカウントすることを希望する。これは、使用条件を以下のように作成することになるだろう。

【0226】

【表10】

	使用条件 1	使用条件 2	使用条件 3
圧縮コード化バージョン	384Kbps	384Kbs	56Kbps
ユーザのタイプ	個人消費者	個人消費者	個人消費者
トランザクションのタイプ	購入	賃貸借	購入
使用可能日	1997年10月1日 ～1997年12月31日	1997年10月1日 ～1997年12月31日	1997年10月1日 ～1997年12月31日
国	米国およびカナダ	米国およびカナダ	米国およびカナダ
ウォーターマーク	標準	標準	標準
通知イベント	コピー処置	なし	なし
コピー回数	1	0	0
媒体	ミニディスク	適用不可	適用不可
賃貸借期間	適用不可	14日間	適用不可
価格	価格 1	価格 2	価格 3

【0227】4. メタデータSC620の各パーツ
メタデータSC620に含めるためにメタデータ同化入
カツール161が収集するデータの種類の一部を以下に＊
製品ID

ライセンス許諾者レコード会社

ライセンス保持者レコード会社

このオブジェクト（二次ライセンス保持者レコード会社）のソース（発行者）

【0228】

〔ソース：コンテンツ・プロバイダ〕

〔宛先：全員；〕

〔宛先：EMS；エンドユーザ；〕

〔宛先：EMS；エンドユーザ；〕

〔宛先：全員；〕

オブジェクトのタイプ（すなわち、単一オブジェクトまたは複数オブジェクト
のアレイ）

オブジェクトID

〔宛先：全員；〕

国際標準記録コード（ISRC）

国際標準音楽番号（ISMN）

使用条件（ソース：コンテンツ・プロバイダ；宛先：EMS、エンドユーザ、ク
リアリング・ハウス105）

購入済み使用条件（ソース：EMS；宛先：エンドユーザ、クリアリング・ハウ
ス105）

オブジェクト（録音）の使用のための使用条件のセット（消費者の制限および
権利）

使用条件のアレイ内の個々の項目

この使用条件が適用されるコンテンツ113の圧縮コード化バージョン

この使用条件がコンテンツ113の購入を可能にするか賃貸借を可能にする
か

賃貸借トランザクションの場合：

賃貸借の期間を限定するために使用する測定単位（たとえば、日数、
再生回数）

それ以降コンテンツ113がもはや再生されなくなる上記の単位数

購入トランザクションの場合：

エンドユーザが作成を許される再生可能コピーの数

コピーを作成可能な媒体の種類（たとえば、CDレコーダブル（CD
-R）、ミニディスク、パーソナル・コンピュータ）

購入／賃貸借トランザクションを行える期間（すなわち、エンドユーザは
、使用可能開始日後であってしかも使用可能最終日前に限り、この使用条件の条
件下で購入／賃貸借を行うことができる）

エンドユーザがこの購入（または賃貸借）のトランザクションを行うこと
ができる国を指し示すポイント

この使用条件下での購入／賃貸借トランザクションの価格

暗号化ウォーターマーク命令およびパラメータを指し示すポイント

クリアリング・ハウス105の通知を必要とするイベントのタイプを指し示すポインタ

購入データ (暗号化; 任意選択情報; ソース: EMS; 宛先: エンドユーザ、クリアリング・ハウス105)

購入日

購入価格

請求先の名前と住所

消費者の名前と住所

消費者の国 (最良推測)

メタデータ1 (ソース: コンテンツ・プロバイダ; 宛先: EMS、エンドユーザ)

アレイ {

著作権情報

作曲の場合

録音の場合

歌曲のタイトル

主要アーティスト

}

ポインタ {

アートワーク (たとえば、アルバム・カバー)

アートワークのフォーマット (たとえば、GIF、JPEG)

}

任意選択情報:

追加情報のアレイ {

作曲家

発行者

プロデューサ

伴奏楽器奏者

録音日

リリース日

歌詞

トラック名 (説明) / トラック長

この録音が収録されたアルバムのリスト

ジャンル

}

メタデータ2 (ソース: コンテンツ・プロバイダ; 宛先: EMS)

複数構造のアレイ、それぞれは同じ録音の異なる品質レベルを表す {

録音;

録音の品質レベル;

(おそらく圧縮された) 録音のサイズ (バイト単位)

}

メタデータ3 (ソース: コンテンツ・プロバイダ; 宛先: EMS、エンドユーザ)

任意選択情報:

プロモーション素材:

アーティスト・プロモーション素材を指し示すポインタ {

アーティストのウェブ・サイトへのURL;

アーティストの背景説明;

アーティスト関連インタビュー (インタビューのフォーマット (たとえば、テキスト、オーディオ、ビデオ) 付き);

評論（評論のフォーマット（たとえば、テキスト、オーディオ、ビデオ）

付き）；

サンプル・クリップ（およびそのフォーマットと圧縮レベル）；

最近および今後のコンサート／出演／イベント — それぞれの日付および場所；

）

アルバム・プロモーション素材を指し示すポインタ（

サンプル・クリップ（およびそのフォーマットと圧縮レベル）；

プロデューサまたは作曲家、映画／演劇／配役、アルバム作成などの背景

説明；

非アーティスト関連インタビュー（インタビューのフォーマット（たとえば、テキスト、オーディオ、ビデオ）付き）；

評論（評論のフォーマット（たとえば、テキスト、オーディオ、ビデオ）

付き）；

ジャンル；

）

シングル・プロモーション；

サンプル・クリップ（およびそのフォーマットと圧縮レベル）

プロデューサまたは作曲家、映画／演劇／配役、シングル作成などの背景

説明；

評論（評論のフォーマット（たとえば、テキスト、オーディオ、ビデオ）

付き）

【0229】5. 監視付きリリース・ツール

監視付きリリース・ツールは、前述の監視付きリリース・プロセス806を実施する能力をユーザに提供する。監視付きリリース権限を有するものとしてコンテンツ・プロバイダ101が指定した個人は、監視付きリリースを待っている製品（すなわち、監視付きリリース・プロセス806の待ち行列上にある製品）を呼び出し、そのコンテンツ113とその付随コメントを検査し、以下のいずれかを行うことができる。そのコンテンツ113を承認し、メタデータSC620にバックするためにその製品をリリースするか、必要な訂正を加え、メタデータSC620にバックするためにその製品をリリースするか、実行すべき訂正アクションを指定するコメントを追加し、手動メタデータ入力プロセス704に製品を再提示する。

【0230】他の実施形態には、SCの作成後、もう1つの任意選択の品質保証ステップが存在し、そこではSCのコンテンツ113をオープンし、完璧さおよび正確さについて検査することができ、その時点で、小売経路へのその製品のリリースについて最終承認を与えるかまたは拒否することができる。

【0231】D. コンテンツ処理ツール

コンテンツ処理ツール155は、実際には、デジタル・コンテンツ・ファイルを処理し、コンテンツのウォーターマーク付きコード化暗号化コピーを作成するために使用するソフトウェア・ツールの集合である。これらのツールは、業界標準のデジタル・コンテンツ処理ツールを利用し、ウォーターマーク、コード化、および暗号化の

諸技術が進化するにつれてその技術を差込み交換できるようにする。選択した業界ツールがコマンド行システム呼び出しインタフェースによりロードされ、それにパラメータを渡すことができるか、またはDLLインタフェースにより関数を呼び出すことができるツールキットを提供する場合、そのコンテンツ処理はある程度まで自動化することができる。各ツールへのフロントエンド・アプリケーションは、次の使用可能なジョブについてコンテンツ処理ツール155内の適切な待ち行列に照会し、必須ファイルおよびパラメータを取り出し、業界標準のコンテンツ処理ツールをロードして必須関数を実行する。そのタスクが完了すると、そのツールが終了状況を報告しない場合、待ち行列への手動更新が必要になる場合もある。

【0232】コンテンツ処理ツール155の汎用バージョンについて説明するが、カスタマイズも可能である。コンテンツ処理ツール155は、Java、C/C++、それと同等のソフトウェアで作成することができる。また、コンテンツ処理ツール155は、ディスク、CDを含むコンピュータ可読手段あるいはウェブ・サイトにより送達することができる。

【0233】1. ウォータマーク・ツール

ウォータマーク・ツールは、前述のウォータマーク・プロセス808を実施する能力をユーザに提供する。このツールは、オーディオ・ウォータマーク技術を使用して歌曲ファイルにコンテンツ113のオーナーの著作権情報を適用する。書き出される実際の情報は、コンテンツ・プロバイダ101と、選択した特定のウォータマーク技

術によって決定される。この情報は、それがこの情報をウォータマーク機能に適切に渡すことができるように、フロントエンド・ウォータマーク・ツールにとって使用可能なものである。これは、たとえば、歌曲のオーディオ・ファイルを処理できるようにする前にこの情報を取得したことを保証するために、メタデータ同化入力ツール161に同期要件を課すものである。この歌曲は、ウォータマーク情報が入手されるまで、オーディオ処理に使用可能な状態にならない。

【0234】ウォータマークは、作成した歌曲のすべてのコード化に共通なものなので、オーディオ処理の第1のステップとして適用される。ウォータマークがコード化技術以降も存続可能な限り、ウォータマーク・プロセスは1曲につき1回だけ行えばよい。

【0235】様々なウォータマーク技術が知られており、市販されている。しかし、フロントエンド・ウォータマーク・ツールは、様々な業界用ウォータマーク・ツールをサポートすることができる。

【0236】2. 前処理圧縮ツール

前処理圧縮ツールは、前述の前処理圧縮プロセス809を実施する能力をユーザに提供する。オーディオ・コード化は2つのプロセスを必要とする。コード化は、基本的に、音楽コンテンツの例の場合はPCMオーディオ・ストリームに対して損失圧縮アルゴリズムを適用することである。通常、エンコーダは、必要なオーディオ品質のレベルに基づいて様々な再生ビット・ストリーム・レートを生成するように調整することができる。品質が高くなると結果的にファイル・サイズが大きくなり、高品質コンテンツ113の場合、ファイル・サイズは非常に大きいものになる可能性がある。高品質コンテンツ113のダウンロード時間は長々しく、時には標準の28800bpsモデム上で非常に高いものになる可能性がある。

【0237】したがって、コンテンツ・プロバイダ101は、1回のダウンロードのために何時間も待ちたくない性急で低帯域幅の顧客と、高品質コンテンツ113のみを購入するかより高速の接続を有するオーディオファンまたは広帯域幅の顧客の両方をなだめるために、ダウンロード用に様々なデジタル・コンテンツ品質を提示することを選ぶことができる。

【0238】圧縮アルゴリズムは、コンテンツ113を低ビット伝送速度で複製するためのそれぞれの技術が異なる。この技術は、アルゴリズムごと（すなわち、MP3、AC3、ATRAC）および圧縮レベルごとに異なる。より高レベルの圧縮を達成するために、通常、データは、圧縮アルゴリズムに送達される前により低いサンプリング速度で再サンプリングされる。忠実度の損失が低く、より効率の良い圧縮を可能にするために、またはいくつかの周波数範囲の激しいドロップアウトを防止するために、デジタル・コンテンツは、所与の周波数

の等化レベルに応じた調整または録音の強弱の変化に応じた調整を必要とする場合もある。コンテンツの前処理要件は、圧縮アルゴリズムおよび必要な圧縮のレベルに直接関連する。場合によっては、コンテンツ113のスタイル（たとえば、音楽ジャンル）は前処理要件を決定するためのベースとして正常に使用することができる。というのは、同じジャンルの複数の歌曲は通常、同様の強弱の変化を有するからである。一部の圧縮ツールでは、このような前処理機能はコード化プロセスの一部である。他のツールでは、圧縮の前に所望の前処理が実行される。

【0239】販売用のダウンロード可能なオーディオ・ファイルに加え、各歌曲は、低ビット伝送速度（LBR）コード化クリップも有し、その歌曲をLBRストリーミング・プロトコルによってサンプリングできるようにする。このLBRコード化はコンテンツ処理ツール155の責任でもある。このクリップは、個別のPCMファイルとしてまたはオフセットと長さのパラメータとしてコンテンツ・プロバイダ101によって提供される。

【0240】ウォータマークの場合のように、コード化ツールがDLLまたはコマンド行システム呼出しインタフェースによりロード可能であり、前処理および圧縮のためのすべての必須パラメータが渡されることが期待される。フロントエンド・コード化ツールは、たとえば、コンテンツが音楽であり、オーディオ前処理を実行する前にその歌曲のジャンルがコンテンツ・プロバイダのデータベース160から取得されると判定された場合、メタデータ同化入力ツール161との同期要件を有する可能性がある。これは、選択したコード化ツールと、その歌曲のジャンルがどのように不確定であるかによって決まる。コンテンツ・プロバイダ101が1曲あたりのコード化品質レベルの選択を変更する場合、この情報もコード化ステップの前に提供され、メタデータ同化入力ツール161によって生成されるメタデータと一致する。

【0241】今日、様々な高品質コード化アルゴリズムおよびツールが知られている。しかし、フロントエンド・コード化ツールは、様々な業界用コード化ツールをサポートすることができる。

【0242】次に図15に移行すると、本発明により図11の自動メタデータ収集ツール用の一実施形態の流れ図が示されている。このプロセスは、コンテンツ・プロバイダ101が検査する媒体から識別子を読み取ることから始まる。コンテンツの一例はオーディオCDの実施形態である。オーディオCDの実施形態では、ユニバーサル価格コード（UPC）、国際標準記録コード（ISRC）、国際標準音楽番号（ISMN）というコードが使用可能である可能性がある。ステップ1201で、コンテンツ用の適切なプレーヤ、たとえば、オーディオCD用のオーディオCDプレーヤ、DVD映画用のDVDプレーヤ、DAT録音用のDATレコーダ、およびそれ

と同等のものでこの識別子を読み取る。次に、ステップ1202で、この識別子を使用してコンテンツ・プロバイダ101用のデータベース160に索引を付ける。ステップ1203では、図11に記載したようにワーク・フロー・マネージャ・プロセスが必要とする情報の一部または全部をデータベース160およびその他の関連ソースから取り出す。この情報は、コンテンツ113と、それに関連するメタデータを含むことができる。ステップ1204では、取り出した追加情報を使用して、電子コンテンツ113を作成するためにワーク・フロー・マネージャ154を開始する。ただし、自動メタデータ収集ツールが電子配布のために一連のコンテンツ113を作成できるように、複数のオーディオCDなど、複数媒体の選択肢を待ち行列化することによって留意されたい。たとえば、すべてのコンテンツ113は、一連のCDまたはコンテンツ・プロバイダ101が検査した1つまたは複数のCDから選択したトラックから作成することができるだろう。

【0243】代替実施形態では、コンテンツ・プロバイダのデータベース160から自動的に前処理パラメータを取り出すことができる。次に図16を参照すると、本発明により図11の前処理圧縮ツールの前処理圧縮パラメータを自動的に設定するための方法の流れ図が示されている。この実施形態のコンテンツ113は音楽である。ステップ1301では、コンテンツ処理ツール155でコード化すべき音楽（コンテンツ113）を選択する。ステップ1302では、選択した音楽のジャンルを決定する。これは、手動で入力するかまたは図15に記載したプロセスから取り出した追加データなど、他の使用可能なメタデータを使用することにより入力することができる。次にステップ1303では、選択したオーディオ圧縮レベルおよびオーディオ圧縮アルゴリズムを検査する。次にステップ1304では、ジャンルによって、ルックアップを行い、前処理圧縮プロセス809でどの圧縮パラメータを使用すべきかについての圧縮設定および圧縮アルゴリズムを選択する。

【0244】3. コンテンツ品質管理ツール
コンテンツ品質管理ツールは、前述のコンテンツ品質管理プロセス810を実施する能力をユーザに提供する。これは、任意選択のコンテンツ処理ツールであり、品質管理専門家がコード化しウォーターマークを付けたコンテンツ・ファイルを検討し、品質判断に基づいてそのコンテンツ・ファイルを承認または拒否するための機会を提供する。その専門家は、その品質が妥当なものになるまで手動前処理調整を行ってそのコンテンツを再コード化することができ、あるいは再処理用のフラグをその歌曲に付け、問題を記述する注を付加することができる。

【0245】このプロセス・ステップは、コンテンツ処理ワーク・フローの任意選択ステップまたは必須ステップとしてコンテンツ・プロバイダ101が構成すること

ができる。このコンテンツ用のすべてのSC（たとえば、1枚のCD上の複数歌曲用の各SC）のパッケージ化後に、最終品質保証プロセス813の追加かつ任意選択のステップが用意されており、その時点でコンテンツ・コード化の品質をテストすることができるが、暗号化およびパッケージ化の前に早めに問題を把握すると、より効率の良いコンテンツ処理が可能になる。したがって、すべての処理の最終完了まで待つことは対照的に、このステップでコンテンツ品質を保証することは非常に望ましいことである。

【0246】4. 暗号化ツール

暗号化ツールは、前述の暗号化プロセス811を実施する能力をユーザに提供する。コンテンツ暗号化はコンテンツ処理ツール155の最終ステップである。コード化ツールによって作成されたコンテンツの各バージョンをここで暗号化する。暗号化ツールはSCバックカ機能の1つである。SCバックカを呼び出して歌曲を暗号化し、使用した生成暗号化キーを返す。その後、このキーは、メタデータSC620の作成時に使用するためにSCバックカに渡される。

【0247】E. コンテンツSC作成ツール

すべてのメタデータが収集されると、コンテンツSC作成ツールはそれぞれの所期の用途に基づいてそのメタデータをカテゴリ別にグループ化する。これらのメタデータ・グループは、メタデータSC620用のメタデータ・パーツとしてSCバックカ・ツールに渡されるファイル内に作成される。各パーツ（ファイル）は固有の処理要件を有する。関連歌曲が処理され暗号化され、ターゲット宛先（コンテンツ・ホスト・サイト111のURL）が決定されると、コンテンツ113用のコンテンツSC630はいつでも作成できる状態になる。処理が完了し、前述のすべての要件を満たしたコンテンツ113は、ワーク・フロー・マネージャ154のバック待ち行列にバックするために待ち行列化される。

【0248】次にコンテンツSC作成ツールは、メタデータ同化入力ツール161の先行ステップによって作成されたすべての必須ファイルを取り出し、SCバックカ機能呼び出してメタデータSC620およびコンテンツSC630を作成する。このプロセスは、各歌曲ごとに単一のメタデータSC620と複数のコンテンツSC630を作成する。たとえば、コンテンツが音楽である場合、歌曲全体の様々な品質レベルに関するオーディオ処理中に作成した各オーディオ・ファイルを別々のコンテンツSC630にバックする。サンプル・クリップ用に作成したオーディオ・ファイルは、メタデータSC620に含めるメタデータ・ファイルとして渡される。

【0249】F. 最終品質保証ツール

最終品質保証ツールは、前述の最終品質保証プロセス813を実施する能力をユーザに提供する。1つのコンテンツ・ファイルについてすべてのSCが構築されると、

そのコンテンツは最終品質保証チェックに使用可能な状態になる。品質保証は、コンテンツ113の作成プロセスの様々な段階で実行することができる。コンテンツ・プロバイダ101は、その後の過度の手直しを防止するために各主要ステップが完了するたびに品質保証を実行することを選択することができ、あるいはすべてのオーディオ作成プロセスが完了するまで待ち、すべてについて一度に品質保証を実行することを選択することもできる。後者を選択した場合、SCの作成が完了すると、この時点で品質保証が実行される。このツールにより、その歌曲用の各SCをオープンして検査し、オーディオ再生することができる。

【0250】いずれかの問題が検出されると、わずかなテキスト変更でも、SCの内部セキュリティ機構によりSCを再構築しなければならない。不必要な再処理時間を回避するため、暫定品質保証ステップを使用してメタデータの正確さを保証することと、この歌曲に関連するSC間の適切な相互参照を妥当性検査するためにこの特定の品質保証ステップを予約することが非常に推奨される。問題が検出された場合、保証者は、歌曲に付加すべき問題記述を入力し、それを再処理のために適切な処理待ち行列に再待ち行列化することができる。歌曲のすべての関連コンポーネントの状況を示すように、ワーク・フロー・マネージャ154内で適切に状況を更新する。いかなる問題も検出されない場合、コンテンツ113にはリリース可能を示すマークまたはフラグが付けられる。

【0251】G. コンテンツ分散ツール

コンテンツ分散ツールは、前述のコンテンツ分散プロセス814を実施する能力をユーザに提供する。リリースのためにコンテンツ113が承認されると、コンテンツ113用のSCはコンテンツ分散プロセスの待ち行列内に置かれる。コンテンツ分散ツールは待ち行列を監視し、コンテンツ・プロバイダ101によって提供された構成設定に基づいてSCファイルの即時転送または1群のSCファイルのバッチ転送を実行する。また、コンテンツ・プロバイダ101は任意選択で、リリースのために手動でフラグが付けられるまですべてのSCをこの待ち行列内に自動的に保持するようにコンテンツ分散ツールを構成することもできる。これにより、コンテンツ・プロバイダ101は、スケジューリングしたリリース日に先だってコンテンツを作成し、たとえば、新しい歌曲、映画、またはゲームなど、それをリリースしたいと希望するようになるまでそれを保持することができる。また、SCは定義済みリリース日に基づいてコンテンツ113へのアクセスを制御することもできるので、コンテンツ・プロバイダ101が実際にSCの送達を止めるための要件は一切存在しないが、この手動リリース・オプションは依然としてこの目的に使用するかまたはこれらの大型ファイルを転送するために必要なネットワーク

帯域幅を管理するために使用することができる。

【0252】リリースのためにフラグが付けられると、コンテンツ113用のコンテンツSC630はFTPにより指定のコンテンツ・ホスト・サイト111に転送される。メタデータSC620はFTPによりコンテンツ・プロモーション・ウェブ・サイト156に転送される。この場合、SCは、処理し、コンテンツ・プロモーション・ウェブ・サイト156に統合できるようになるまで、コンテンツ113の新しいディレクトリにステージングされる。

【0253】図21は、本発明により図11の自動メタデータ収集ツール用の追加情報を自動的に検索するための代替実施形態の流れ図である。このプロセスは、上記の図11に記載したものと同様のものである。しかし、監視付きリリース806およびコンテンツ品質管理809の品質チェックは、品質管理1704という1つの品質チェックに結合されている。メタデータSC作成807およびコンテンツSC作成812の前に品質チェックを実行する。SC作成の前に品質チェックを実行すると、コンテンツ113および関連メタデータSC620をアンパックするステップが除去される。そのうえ、この実施形態では、製品待受けアクション／情報801の待ち行列が除去されている。ジョブは、どのアクションが要求されているかに応じて、特定のプロセス待ち行列上に置かれる。たとえば、そのジョブが手動メタデータ、すなわち、追加メタデータの入力を必要とする場合、そのジョブは手動メタデータ入力待ち行列上に置かれる。また、自動メタデータ収集803は、メタデータ同化入力ツール161およびコンテンツ処理ツール155より前に前もって行われるように、新コンテンツ要求と併合されている。最後に、使用条件804が自動メタデータ収集803と手動メタデータ入力803時の両方で入力されることを指摘しておくことは重要なことである。その後、使用条件の多くは自動メタデータ収集803のステップ中に自動的に記入することができる。

【0254】H. コンテンツ・プロモーション・ウェブ・サイト

コンテンツ・プロバイダ101がデジタル・ダウンロードにより販売用に使用可能にするものに関する情報を最も効果的に分散するために、また、それがこのコンテンツ113をその顧客へのダウンロード用に使用可能な状態にすることができるように電子デジタル・コンテンツ・ストア103に必要なファイルを取得するために、各コンテンツ・プロバイダ101は、この情報を収容する安全なウェブ・サイトを持っていなければならない。これは、この情報を必要とするその小売業者およびその他のものに対してプロモーション・コンテンツを使用可能な状態にするために、現在、一部のコンテンツ・プロバイダ101が使用する方法と同様のものである。このタイプのサービスがすでに存在する場合、電子ディ

ジタル・コンテンツ・ストア103がダウンロードにより販売用に使用可能なコンテンツのリストを見に行けるような追加のセクションをそのウェブ・サイトに追加することができる。

【0255】コンテンツ・プロバイダ101は、このサイトの設計およびレイアウトを完全に制御しているか、またはセキュア・デジタル・コンテンツ電子配布システム100用のツールキットの一部として提供されるターンキー・ウェブ・サーバ・ソリューションの使用を選択することができる。このサービス用のそれぞれの設計を実施するために、コンテンツ・プロバイダ101は、それぞれのサイトにアクセスする電子デジタル・コンテンツ・サーバ103用のメタデータSC620へのリンクを用意するだけでよい。これは、セキュア・デジタル・コンテンツ電子配布システム100用のツールキットを使用して実施される。この選択プロセスおよびどの情報が示されるかは、コンテンツ・プロバイダ101の自由裁量である。

【0256】コンテンツ分散ツールからFTPにより新しいコンテンツ・ディレクトリ内に受け取ったメタデータSC620は、コンテンツ・プロモーション・ウェブ・サイト156によって処理される。これらのコンテンツは、コンテンツから情報を表示または抽出するためにSCブリビュー・ツールによってオープンすることができる。次に、この情報を使用して、HTMLウェブ・ページを更新するかまたはこのサービスによって維持されるサーチ可能データベースに情報を追加することができる。SCブリビュー・ツールは、実際には、メタデータSC620をオープンして処理するために電子デジタル・コンテンツ・ストア103が使用するコンテンツ収集ツールのサブセットである。詳細についてはコンテンツ収集ツールの項を参照されたい。次に、メタデータSC620ファイルは、コンテンツ・プロモーション・ウェブ・サイト156によって維持される永続ディレクトリに移動しなければならない。

【0257】メタデータSC620がコンテンツ・プロモーション・ウェブ・サイト156に統合されると、その可用性が公表される。コンテンツ・プロバイダ101は、それぞれの新しいメタデータSC620がそのサイトに追加されるたびにすべての加入電子デジタル・コンテンツ・ストア103に通知を送ることができる、あるいはその日（または期間）に追加されたすべてのメタデータSC620に関する単一通知を毎日（またはいずれかの定義済み周期で）実行することができる。この通知は、追加されるメタデータSC620を参照するパラメータを含む定義済みCGIストリングを送ることにより、電子デジタル・コンテンツ・ストア103ウェブ・サーバとの標準のHTTP交換により実行される。このメッセージは、後述する電子デジタル・コンテンツ・ストア103の通知インタフェース・モジュールによ

って処理される。

【0258】1. コンテンツ・ホスト

エンターテインメント業界は、毎年、CD、映画、ゲームなど、何千ものコンテンツ・タイトルを制作し、現在入手可能な何万ものコンテンツ・タイトルをさらに増大させている。セキュア・デジタル・コンテンツ電子配布システム100は、現在、店頭で入手可能なすべてのコンテンツ・タイトルをサポートするように設計されている。

10 【0259】最終的にセキュア・デジタル・コンテンツ電子配布システム100が毎日、顧客に対してダウンロード可能なコンテンツ・タイトルの数は数千または数万である。タイトルが多数の場合、これは大量の帯域幅を必要とする。このようなコンピュータ・ディスク空間および帯域幅の必要性により、複数のコンテンツ・ホスト・サイト111による分散スケーラブル実施が要求される。また、このシステムは、世界中の顧客をサポートする。このため、全世界に渡る顧客への送達を促進するために海外サイトが必要になる。

20 【0260】セキュア・デジタル・コンテンツ電子配布システム100上のコンテンツ・ホストは、コンテンツ・プロバイダ101がそれ自身のコンテンツ113のホストとなるかあるいは1つの共通設備または1組の設備を共用することができるように設計されている。

【0261】セキュア・デジタル・コンテンツ電子配布システム100上のコンテンツ・ホストは、セキュア・デジタル・コンテンツ電子配布システム100によって提供されるコンテンツ113のすべてをひとまとめにして含む複数のコンテンツ・ホスト・サイト111
30 と、コンテンツ・プロバイダ101によって提供される現行ホット・ヒットを含む複数の2次コンテンツ・サイト（図示せず）からなる。コンテンツ・ホスト・サイト111の数は、このシステムを使用するエンドユーザの数に応じて変化する。2次コンテンツ・サイトは限られた数の歌曲のホストとなるが、このシステム上で使用する帯域幅の多くの部分を表すことになる。2次サイトは、1次サイト上のボリュームが最大容量の点まで増大するとオンラインになる。2次サイトはネットワーク・アクセス・ポイント（NAP）付近に位置することができ、これはダウンロード時間を加速するのに役に立つ。また、2次サイトは、ダウンロード時間を加速するために世界中の様々な地域に配置することもできる。

40 【0262】コンテンツ・プロバイダ101がそれ自体のシステム内のすべてのコンテンツ113のホストとなることを選択した場合、追加の2次コンテンツ・サイトの有無にかかわらず、単一のコンテンツ・ホスト・サイト111として動作することができる。このため、それ自体のスケーラブル分散システムを構築することができる。他の実施形態では、電子デジタル・コンテンツ・ストア103も所与のコンテンツ113用のコンテンツ

・ホスト・サイト111として動作することができる。
この実施形態では、電子デジタル・コンテンツ・ストア103とコンテンツ・プロバイダ101との間の特別な財政上の合意が必要である。

【0263】1. コンテンツ・ホスト・サイト

コンテンツ113は、本明細書のコンテンツ・プロバイダの項で説明したコンテンツ分散ツールによるFTPまたはHTTPによるかあるいはテープ、CD-ROM、フラッシュ、その他のコンピュータ可読媒体上でのコンテンツ送達などのオフライン手段により、コンテンツ・ホスト・サイト111に追加される。コンテンツ・プロバイダ101によって作成されたメタデータSC620は、このコンテンツ113用のコンテンツSC630を突き止めるURLを示すフィールドを含む。このURLはコンテンツ・ホスト・サイト111に対応する。電子デジタル・コンテンツ・ストア103は、コンテンツ・プロバイダ101によって許される場合、オファースC641内でこのURLを指定変更することができる。エンドユーザ装置109は、コンテンツSC630をダウンロードしたいと希望する場合、このコンテンツ・ホスト・サイト111に連絡する。

【0264】エンドユーザ装置109は、コンテンツ・ホスト・サイト111にライセンスSC660を送ることにより、コンテンツSC630を求める要求を開始する。これは、クリアリング・ハウス105によって返されるのと同じライセンスSC660である。ライセンスSC660のデジタル・シグニチャを検証すると、それが有効なライセンスSC660であるかどうかを判定することができる。それが有効なライセンスSC660である場合、ダウンロードが開始されるかまたはダウンロード要求を他のコンテンツ・ホスト・サイト111にリダイレクトすることができる。

【0265】2. セキュア・デジタル・コンテンツ電子配布システム100によって提供されるコンテンツ・ホスト・サイト111

セキュア・デジタル・コンテンツ電子配布システム100の場合、どのサイトを使用してコンテンツ113をダウンロードするかという判断は、コンテンツSC630を求める初期要求を受け取った1次コンテンツ・サイトによって行われる。このサイトでは以下の情報を使用してこの判断を行う。

・要求したコンテンツ113のホストとなる2次コンテンツ・サイトが存在するか。(セキュア・デジタル・コンテンツ電子配布システム100によって提供されるコンテンツ113の大部分は1次サイトにのみ位置する。)

・エンドユーザ装置109は地理的にどこに位置するか。(この情報は、その要求がエンドユーザ装置109で開始されたときにはエンドユーザ装置109から入手することができ、これはオーダSC650に入れてクリ

アリング・ハウス105に渡される。)

・適切な2次サイトが機能しているか。(場合によっては、2次サイトがオフラインになっている可能性がある。)

・2次サイトの負荷は何か。(2次サイトが活動責めにあっている場合、あまり混んでいない他のサイトを選択することもできる。)

【0266】エンドユーザ装置109にコンテンツSC630を伝送する前に、エンドユーザの要求で分析および検証が行われる。コンテンツ113をダウンロードするために使用したすべてのライセンスSC1Dのデータベースを保持する。このデータベースをチェックして、エンドユーザ装置109が購入したコンテンツ113の各ピースごとに1つの要求のみ行うことを保証することができる。このため、悪意のあるユーザは、コンテンツ・ホスト・サイト111の速度低下を期待してコンテンツ・ホスト・サイト111に繰返しアクセスすることができなくなり、コンテンツSC630の無許可ダウンロードが防止される。

【0267】2次コンテンツ・サイトへのコンテンツ113のプロモーションとデモーションは、コンテンツ113の個々のピースに対する顧客の需要に基づいて定期的に行われる。

【0268】コンテンツ・ホスト・ルータ

コンテンツ・ホスト・ルータ(図示せず)は、コンテンツ・ホスト・サイト111内に存在し、コンテンツ113をダウンロードしようと待っているエンドユーザからのすべての要求を受け取る。このルータは、エンドユーザの要求に対する妥当性検査を実行し、そのエンドユーザが本当にコンテンツ113を購入したことを保証する。どのコンテンツ113がそこに存在するかとその現行状況を含む、2次コンテンツ・サイトの状況に関するデータベースが維持される。この現行状況としては、そのサイト上での活動量と、サイトがメンテナンスのために停止しているかどうかを含む。

【0269】コンテンツ・ホスト・ルータへの唯一のインタフェースはライセンスSC660であり、このSCはコンテンツ113をダウンロードする必要があるときにエンドユーザ装置109によって送られる。ライセンスSC660は、そのユーザがコンテンツ113をダウンロードできることを示す情報を含む。

【0270】2次コンテンツ・サイト

2次コンテンツ・サイト(図示せず)は、セキュア・デジタル・コンテンツ電子配布システム100の人気のあるコンテンツ113のホストとなる。これらのサイトは、地理的には世界中に分散し、ダウンロード時間を改善するためにネットワーク・アクセス・ポイント(NAP)付近に位置する。これらのサイトは、1次コンテンツ・ホスト・サイト111での需要に応じて最大容量付近までシステムに追加される。

【0271】IX. 電子デジタル・コンテンツ・ストアA. 概要—複数電子デジタル・コンテンツ・ストア103のサポート

電子デジタル・コンテンツ・ストア103は本質的に小売業者である。これは、顧客に配布すべきコンテンツ113をマーケティングするエンティティである。コンテンツ113の配布の場合、これは、デジタル・コンテンツ小売ウェブ・サイト、デジタル・コンテンツ小売ストア、または顧客への電子コンテンツ113のマーケティングにかかわりたいと希望する企業を含むことになるだろう。これらの企業は電子コンテンツ113のみの販売をマーケティングすることができるかまたは現在、販売のために提供しているその他の商品に電子商品の販売を追加することを選択することができる。ダウンロード可能な電子商品を電子デジタル・コンテンツ・ストア103のサービス・オファリングに取り入れることは、セキュア・デジタル・コンテンツ電子配布システム100の一部として電子デジタル・コンテンツ・ストア103用に開発された1組のツールにより実施される。

【0272】このようなツールは、以下の動作のために電子デジタル・コンテンツ・ストア103が使用する。

- ・ コンテンツ・プロバイダ101によってパッケージ化されたメタデータSC620を取得する。
- ・ これらのSCからコンテンツ113を抽出して、そのサービス・オファリングを構築するための入力として使用する。
- ・ 販売のために提供するダウンロード可能なコンテンツ113を記述するオファーSC641を作成する。
- ・ トランザクションSC640を作成してエンドユーザ装置109に送ることにより、販売の肯定応答およびダウンロードの開始を処理する。
- ・ ダウンロード可能なコンテンツ113の販売と各ダウンロードの状況を示すトランザクション・ログを管理する。
- ・ 状況通知およびトランザクション認証要求を処理する。
- ・ 会計調停を実行する。

【0273】これらのツールは、電子デジタル・コンテンツ・ストア103がダウンロード可能な電子コンテンツ113の販売をそのサービスに統合したいと希望する際に柔軟性を見込むように設計されている。これは必須ではないが、購入したダウンロード可能なコンテンツ113に関するすべての金融決済がクリアリング・ハウス105によって処理されることを要求するように、これらのツールを使用することができる。また、これらのツールは、電子デジタル・コンテンツ・ストア103がその顧客に完全に対応し、プロモーションおよび特殊オファターの提供を含む、金融トランザクション自体を処

理できるようにする。これらのツールは、電子デジタル・コンテンツ・ストア103がダウンロード可能なコンテンツ113の販売をその既存サービスに迅速に統合できるようにする。そのうえ、電子デジタル・コンテンツ・ストア103は、ダウンロード可能なコンテンツ113のホストとなる必要がなく、その分散を管理する必要もない。この機能は、コンテンツ・プロバイダ101が選択したコンテンツ・ホスト・サイト111によって実行される。

【0274】電子デジタル・コンテンツ・ストア103用のツールは、好ましい実施形態ではJavaで実現されているが、C/C++、アセンブラ、それと同等のものなど、他のプログラミング言語も使用することができる。ただし、電子デジタル・コンテンツ・ストア103に関して後述するツールは様々なハードウェアおよびソフトウェア・プラットフォームで動作可能であることに留意されたい。完全なシステムとしてまたはその構成コンポーネントの一部としての電子デジタル・コンテンツ・ストア103は、ウェブなどの電子配布またはフロッピー・ディスク、CD-ROM、取外し可能ハード・ディスク・ドライブを含みかつこれに限定されないコンピュータ可読媒体に入れてアプリケーション・プログラムとして配布することができる。

【0275】他の実施形態では、電子デジタル・コンテンツ・ストア103のコンポーネントはプログラムのソフトウェア・ツールキットの一部である。このツールキットにより、後述する電子デジタル・コンテンツ・ストア103の汎用コンポーネントおよびツールの各種コンポーネントへの事前定義インタフェースが可能になる。このような事前定義インタフェースは、APIまたはアプリケーション・プログラミング・インタフェースの形式になっている。このようなAPIを使用する開発者は、高レベル・アプリケーション・プログラムから各種コンポーネントの機能性のいずれかを実現することができる。このようなコンポーネントにAPIを提供することにより、プログラマは、これらのコンポーネントのいずれかの機能およびリソースを再作成する必要なしに、カスタマイズした電子デジタル・コンテンツ・ストア103を迅速に開発することができる。

【0276】電子デジタル・コンテンツ・ストア103は、ウェブ・ベースのサービス・オファリングに限定されない。提供されるツールは、このコンテンツ113をエンドユーザに送達するために使用する伝送インフラストラクチャまたは送達モードにかかわらず、ダウンロード可能な電子コンテンツ113を販売したいと希望するすべての電子デジタル・コンテンツ・ストア103が使用する。衛星およびケーブル・インフラストラクチャにより提供される同報通信サービスも同じツールを使用して、電子コンテンツ113の販売を取得し、パッケージ化し、追跡する。販売のための電子商品の提示およ

びこれらのオファ―がエンドユーザに送達される方法は、同報通信ベースのサービス・オファリングとポイントツーポイント対話ウェブ・サービス・タイプのオファリングとの間の主な変形である。

【0277】B. ポイントツーポイント電子デジタル・コンテンツ配布サービス

ポイントツーポイントは、主に、電子デジタル・コンテンツ・ストア103とエンドユーザ装置109との間の1対1の対話サービスを意味する。これは、通常、電話またはケーブル・モデム接続によって提供されるインターネット・ウェブ・ベースのサービスを表す。インターネット以外のネットワークも、ウェブ・サーバ/クライアント・ブラウザ・モデルに適合する限り、このモデルでサポートされる。図12は、電子デジタル・コンテンツ・ストア103の主要ツール、コンポーネント、プロセスを示すブロック図である。

【0278】1. 統合要件

セキュア・デジタル・コンテンツ電子配布システム100は、新しいオンライン・ビジネスを創出するだけでなく、既存のビジネスがダウンロード可能な電子コンテンツ113の販売をその現行在庫に統合するための方法も提供する。電子デジタル・コンテンツ・ストア103に提供されるツール一式は、この統合努力を簡略化する。コンテンツ収集ツール171とSCバック・ツール153は、電子デジタル・コンテンツ・ストア103が販売のために使用可能な状態で持っているものに関する情報を参加コンテンツ・プロバイダ101から収集し、このようなダウンロード可能なオブジェクトをそのプロバイダ自体の在庫内の項目として参照するために必要なファイルを作成するための方法を提供する。このプロセスは、バッチ駆動され、大部分は自動化することができ、新しいコンテンツ113をそのサイト内に統合するためにのみ実行される。

【0279】セキュア・デジタル・コンテンツ電子配布システム用のツールは、その現行コンテンツ113小売パラダイムに最小限の変更を加えることにより、ウェブ・ベースの電子デジタル・コンテンツ・ストア103の典型的な実施例（すなわち、Columbia Houseオンライン、Music Boulevard、Tower）およびそれと同等なものにダウンロード可能な電子コンテンツ113の販売を統合できるように設計されている。いくつかの統合方法が可能であり、好ましい実施形態では、電子デジタル・コンテンツ・ストア103はすべての製品サーチ、レビュー、選択（ショッピング・カート）、購入をサポートする。各電子デジタル・コンテンツ・ストア103は、その顧客とともに顧客への忠誠を確立し、それ自体の刺激策を提供し、現在行っているようにその製品のマーケティングを続行する。セキュア・デジタル・コンテンツ電子配布システム100では、その在庫内のどの製品が電子ダウンロードに使用可能であるかを示し、

購入選択を行うときにその顧客が電子ダウンロード・オプションを選択できるようにすることが必要になるだけであろう。他の実施形態では、顧客のショッピング・カートは電子媒体選択（コンテンツ113）と物理媒体選択の混合物を含む可能性がある。顧客がチェックし、電子デジタル・コンテンツ・ストア103が金融決済を完了し、購入した物理的商品を処理するためにその発送処理機能をログ記録するかまたは通知した後、電子デジタル・コンテンツ・ストア103の商取引処理機能はトランザクション・プロセッサ・モジュール175を呼び出してすべての電子ダウンロードを処理する。これは必須情報を渡すだけであり、その時点からのすべての処理はセキュア・デジタル・コンテンツ電子配布システム100用のツールセットによって処理される。他の実施形態では、電子デジタル・コンテンツ・ストア103がダウンロード可能な商品の販売のみを希望するかまたは物理的商品とダウンロード可能な商品の金融決済の分離を希望する場合、金融決済を処理するためにセキュア・デジタル・コンテンツ電子配布システム100用のツールを使用する他のトランザクション処理方法も可能である。

【0280】諸品のダウンロードを処理するために、電子デジタル・コンテンツ・ストア103には、それがコンテンツ・プロバイダ101用のコンテンツ・プロモーション・ウェブ・サイト156から取得するダウンロード可能な各製品ごとに製品ID（図示せず）が与えられる。この製品IDは、ダウンロード可能な製品に対する顧客の購入選択に関連付けられている。製品IDは、ユーザが購入した製品を識別するために電子デジタル・コンテンツ・ストア103がトランザクション・プロセッサ・モジュール175に渡すものである。製品を記述するために作成されたSC（オファ―SC641）は、電子デジタル・コンテンツ・ストア103から分離され、このようなオブジェクトの管理を簡略化し、その存在を電子デジタル・コンテンツ・ストア103にとって透過的なものにしようとして、オファ―・データベース181内に保持される。

【0281】トランザクション・プロセッサ・モジュール175およびその他の追加機能は、ウェブ・サーバ側の実行可能機能（すなわち、CGIおよびNSAPI、ISAPI呼び出し可能機能）または単なるAPIとしてDLLまたはCオブジェクト・ライブラリに用意される。これらの機能は、クリアリング・ハウス105とのエンドユーザ対話および任意選択対話のランタイム処理を取り扱う。これらの機能は、ウェブ・サーバの商取引サービスと対話して、コンテンツ113のダウンロード・プロセスを開始するために必要なファイルを作成し、それをエンドユーザ装置109にダウンロードする。また、これらは、認証を行い、活動の完了通知を受け入れるための任意選択対話も処理する。

111

【0282】それ自体およびクリアリング・ハウス105のトランザクション・ログに基づいて会計を調停するためにクリアリング・ハウス105に連絡する際に電子デジタル・コンテンツ・ストア103を支援するように、会計調停ツール179も用意されている。

【0283】2. コンテンツ収集ツール171

コンテンツ収集ツール171は、メタデータSC620をレビューしダウンロードするためにコンテンツ・プロモーション・ウェブ・サイト156とのインタフェースを担当する。コンテンツ・プロモーション・サイトは標準のウェブ・サイトなので、このサイトをナビゲートするために電子デジタル・コンテンツ・ストア103はウェブ・ブラウザを使用する。ナビゲーション機能は、コンテンツ・プロバイダ101のサイト設計に基づいて様々である。一部のサイトは、多くのプロモーション情報画面によって広範囲なサーチ機能を提供する可能性がある。その他のサイトは、そこから選択するためにタイトル、演奏者、新リリースのリストを備えた単純なブラウザ・インタフェースを有する可能性がある。どのサイトも、1つの歌曲またはアルバムのプロモーション情報および記述情報のすべてを含むメタデータSC620の選択を含んでいる。

【0284】あるいは、電子ストア103は、コンテンツ更新に加入し、FTPにより自動的に更新内容を受け取ることもできる。

【0285】メタデータの閲覧

コンテンツ収集ツール171は、コンテンツ・プロモーション・ウェブ・サイト156でメタデータSC620リンクが選択されたときに必ず立ち上がるウェブ・ブラウザ・ヘルパ・アプリケーションである。そのSCを選択すると、それが電子デジタル・コンテンツ・ストア103にダウンロードされ、ヘルパ・アプリケーションが立ち上がる。コンテンツ収集ツール171はメタデータSC620をオープンし、そこに含まれる非暗号化情報を表示する。表示される情報としては、抽出メタデータ173を含み、音楽の例の場合、その歌曲に関連するグラフィック・イメージとその歌曲を記述する情報を含み、メタデータSC620に含まれていれば、その歌曲のレビュー・クリップも聞くことができる。コンテンツ113が音楽である一例では、コンテンツ・プロバイダ101によって提供されていれば、その歌曲またはアルバムに関するプロモーション情報、アルバム・タイトル、アーティストも示される。この情報は、一連のリンク付きHTMLページとしてブラウザ・ウィンドウに表示される。歌曲や歌詞などの購入可能コンテンツ113と、コンテンツ・プロバイダ101が保護したいと希望するその他のメタデータは、小売コンテンツ・ウェブ・サイト180にとってアクセス不能なものである。

【0286】他の実施形態では、コンテンツ・プロバイダ101は、所定の手数料で任意選択のプロモーション

112

・コンテンツを提供する。この実施形態では、このようなプロモーション・コンテンツはメタデータSC620で暗号化される。このデータをオープンするための金融決済は、指定の手数料が請求される電子デジタル・コンテンツ・ストア103用の口座を備えたクリアリング・ハウス105によって処理することができる。

【0287】メタデータの抽出

レビュー機能に加え、このツールは、メタデータ抽出とオファーSC641の作成という2つの追加機能を提供する。メタデータ抽出オプションを選択すると、電子デジタル・コンテンツ・ストア103は、そのメタデータが記憶されるパスおよびファイル名の入力を要求される。グラフィックおよびオーディオ・レビュー・クリップなどの2進メタデータは別々のファイルとして記憶される。テキスト・メタデータは、小売コンテンツ・ウェブ・サイト180がそのデータベース内にインポート可能なASCII区切りテキスト・ファイルに記憶される。そのASCII区切りファイルのレイアウトを記述するテーブルも個別のTOCファイルに作成される。その他の各国語サポート(NLS)がサポートするフォーマットへの抽出を可能にするために、追加のオプションも使用可能である。

【0288】抽出データとして提供される重要な情報の1つは製品IDである。この製品IDは、ユーザが購入したコンテンツ113をトランザクション・プロセッサ・モジュール175（詳細についてはトランザクション処理の項を参照）に対して識別するために電子デジタル・コンテンツ・ストア103用の商取引処理機能が必要とするものである。トランザクション・プロセッサ・モジュール175はこの製品IDを使用して、エンドユーザ装置109への今後のダウンロードのために適切なオファーSC641をオファー・データベース181から正しく取り出す。電子デジタル・コンテンツ・ストア103は、それがダウンロード可能なコンテンツ113をそのサイト上で提示する方法を完全に制御する。セキュア・デジタル・コンテンツ電子配布システム100用のツールとのインタフェースを適切に取るためには、この製品IDと提供中のコンテンツ113との相互参照を保持することだけが必要である。この情報をここで提供すると、電子デジタル・コンテンツ・ストア103は、オファーSC641の作成プロセスと並行してこの製品またはコンテンツ113をその在庫および販売ページ（データベース）に統合することができる。というのは、どちらのプロセスも、製品を参照するために同じ製品IDを使用するからである。これについては以下に詳述する。

【0289】オファーSC作成バック153

電子デジタル・コンテンツ・ストア103は、販売用のダウンロード可能なコンテンツ113を記述するオファーSC641を作成する必要がある。オファーSC6

41内に入る情報のほとんどはメタデータSC620から導出される。コンテンツ収集ツール171は以下の操作によりオファーSC641を作成する。

- ・ メタデータSC620内でオファーSCテンプレートによって定義されたオファーSC641に含める必要がないパーツをメタデータSC620から除去する。
- ・ 電子デジタル・コンテンツ・ストア103のためにこのツール内の構成オプションで指定されたデフォルトによって定義された追加の必須パーツを追加する。
- ・ メタデータSC620内でオファーSCテンプレートによって定義された追加の必須入力または選択を要求する。
- ・ この情報をSCフォーマットにバックするためにSCバック153を呼び出す。

【0290】エンドユーザ装置109上にプレーヤ・アプリケーション195（以下に詳述する）によって表示されるメタデータはメタデータSC620に保持される。そのウェブ・サービス・データベースへの入力として電子デジタル・コンテンツ・ストア103のみが使用したその他のプロモーション・メタデータはメタデータSC620から除去される。ウォータマーク命令、暗号化対称キー623、そのオブジェクトの許可用途を定義する使用条件517など、コンテンツ・プロバイダ101によって提供される権利管理情報も保持される。

【0291】この余計なものを省いたメタデータSC620はオファーSC641に含まれる。電子デジタル・コンテンツ・ストア103は、ストア使用条件519というそれ自体の使用条件または購入オプションもオファーSC641に付加する。これは、1組のデフォルトにより自動的にまたは対話式に実施することができる。対話式に処理するように構成した場合、電子デジタル・コンテンツ・ストア103は、コンテンツ・プロバイダ101によって定義された1組の許可オブジェクト使用条件517により指示される。次に、そのストアは自分の顧客に対して提供したいオプションを選択する。これらは新しい使用条件またはストア使用条件519になる。自動的に処理するために、電子デジタル・コンテンツ・ストア103は、すべてのコンテンツ113について提供すべき1組のデフォルト購入オプションを構成する。これらのデフォルト・オプションは、コンテンツ・プロバイダ101が定義した許可使用条件517と照らし合わせて自動的にチェックされ、矛盾がなければオファーSC641内に設定される。

【0292】オファーSC641が作成されると、それはオファー・データベース181に記憶され、メタデータSC620で事前割当てされた製品IDで索引が付けられる。この製品IDは、オファー・データベース181とのインタフェースを取り、パッケージ化およびエンドユーザへの伝送のためにオファーSC641を取り出す際に、顧客が購入するダウンロード可能なコンテンツ

113を識別するために後で電子デジタル・コンテンツ・ストア103が使用する。詳細についてはトランザクション・プロセッサ・モジュール175の項を参照されたい。

【0293】他の実施形態では、電子デジタル・コンテンツ・ストア103は自分のサイトでコンテンツSC641のホストとなる。この実施形態では、コンテンツ・ホスト・サイト111のURLを電子デジタル・コンテンツ・ストア103のURLで置き換えるなど、オファーSC641に変更を加える必要がある。

【0294】3. トランザクション処理モジュール175

電子デジタル・コンテンツ・ストア103はクリアリング・ハウス105に請求を振り向ける。あるいは、電子デジタル・コンテンツ・ストア103は、クリアリング・ハウス105から直接、金融決済を要求することができる。ダウンロード可能なコンテンツ113を求めるエンドユーザ購入要求を処理するために、2通りの基本モードが存在する。電子デジタル・コンテンツ・ストア103がその購入の金融決済を処理することを希望せず、その商品の販売を左右する特殊プロモーションまたは刺激策を一切持っておらず、しかも購入要求をバッチ処理するためにショッピング・カート・メタフォーを使用しない場合、そのコンテンツ113ダウンロード・ページ上にオファーSC641ファイルに直接至るリンクを設けることを選ぶことができる。このようなオファーSC641は、メタデータに含まれる小売価格設定情報とともに構築しておく必要があるだろう。また、オファーSC641には、販売の条件とともに購入オプションを提示する特殊HTMLオファー・ページも含まれる。このページは、オファーSC641が構築されたときに作成したテンプレートから構築される。エンドユーザがオファーSC641への直接リンクをクリックすると、オファーSC641はブラウザにダウンロードされ、エンドユーザ装置109はヘルパ・アプリケーションを立ち上げて、コンテナをオープンし、オファーSC641に含まれるオファー・ページを提示する。このページは、クレジット・カード情報および購入オプション選択を含む顧客情報を収集するための書式を含む。この書式は、金融決済および処理のためにクリアリング・ハウス105に直接提示される。任意選択で、この書式は、エンドユーザのクレジット情報または業界標準のローカル・トランザクション・ハンドラを使用するために必要なフィールドを含むことができる。

【0295】次に、電子デジタル・コンテンツ・ストア103が請求を処理する実施形態について説明する。より典型的な購入要求処理モードでは、電子デジタル・コンテンツ・ストア103が金融決済を処理し、ダウンロード認証をエンドユーザに提示することができる。この方法では、電子デジタル・コンテンツ・ストア1

03はダウンロード可能なコンテンツ113の販売とそのサイトで販売するために提供されたその他の商品とを統合することができ、各ダウンロード要求ごとの個別請求ではなく（ショッピング・カート・メタフォーによる）顧客への1回の統合請求のみにより購入要求のバッチ処理が可能になり、電子デジタル・コンテンツ・ストア103がその顧客購入パターンを直接追跡し、特殊プロモーションおよびクラブ・オプションを提供することができる。この実施形態では、ダウンロード可能なコンテンツ113のオファーがそのショッピング・ページに含まれ、それは、エンドユーザが選択したときにショッピング・カートに追加され、電子デジタル・コンテンツ・ストア103の現行ショッピング・モデルで行われるように処理され金融決済される。金融決済が完了すると、電子デジタル・コンテンツ・ストアの商取引処理プロセスはトランザクション・プロセッサ・モジュール175を呼び出して、トランザクションを完了する。

【0296】トランザクション・プロセッサ・モジュール175

トランザクション・プロセッサ・モジュール175の役割は、購入したコンテンツ113のダウンロードを開始し処理するためにエンドユーザ装置109が必要とする情報をまとめることである。この情報は、購入提示に対する応答としてウェブ・サーバによってエンドユーザ装置109に返送されるトランザクションSC640にパッケージ化される。トランザクション・プロセッサ・モジュール175は、電子デジタル・コンテンツ・ストア103の商取引処理プロセスからの3つの情報、すなわち、購入したコンテンツ113用の製品ID、トランザクション・データ642、購入決済を確認するHTMLページまたはCGI URLを必要とする。

【0297】製品IDは、販売したばかりのコンテンツ113に関連するメタデータSC620に入れて電子デジタル・コンテンツ・ストア103に提供される値である。この製品IDは、オファー・データベース181から関連のオファーSC641を取り出すために使用する。

【0298】トランザクション・データ642は、クリアリング・ハウス105の処理を電子デジタル・コンテンツ・ストア103によって実行される金融決済トランザクションと関連させ、エンドユーザ装置109にダウンロードされるコンテンツ113のウォーターマークに含めるユーザ・アイデンティティ情報を提供するために後で使用される電子デジタル・コンテンツ・ストア103のトランザクション処理機能によって提供される情報の構造体である。クリアリング・ハウス105は、有効なオーダSC650を受け取ると、販売されたコンテンツ113、どの電子デジタル・コンテンツ・ストア103がそれを販売したか、エンドユーザの名前およびトランザクションID535を含む関連トランザクション

・データ642を示すトランザクションをログ記録する。トランザクションID535は、金融決済トランザクションへの参照を示す。この情報は、コンテンツ・プロバイダ101（またはそのエージェント）から受け取った請求明細によってその口座を調停する際に使用するために、後でクリアリング・ハウス105によって電子デジタル・コンテンツ・ストア103に返される。クリアリング・ハウス・トランザクション・ログ178は、自分のどのコンテンツ113が販売されたかを判定するためにコンテンツ・プロバイダ101が使用することができる。そのプロバイダはそれが負っている使用料に関し各電子デジタル・コンテンツ・ストア103への請求書を作成することができる。あるいは、請求以外のその他の電子手段を使用して、コンテンツ・プロバイダ101と電子デジタル・コンテンツ・ストア103との間で会計を決済することもできる。

【0299】トランザクションSC640で提供される情報とトランザクションSC640のセキュリティおよび完全性により、購入トランザクションが有効であるという十分な信憑性がクリアリング・ハウス105にもたらされ、したがって、クリアリング・ハウス105によりこの販売をログ記録する前にそれ以上の妥当性検査は不要になる。しかし、電子デジタル・コンテンツ・ストア103は、その口座に請求される前に認証を要求することができる（クリアリング・ハウス105でログ記録されたトランザクションは、この電子デジタル・コンテンツ・ストア103がこのコンテンツ113の販売に関する金銭を集金したことをコンテンツ・プロバイダ101に示す）。認証／通知を求めるこの要求はトランザクション・データ642内のフラグによって示される。このシナリオでは、クリアリング・ハウス105は電子デジタル・コンテンツ・ストア103に連絡し、自分の口座への請求および暗号化キー623のリリースの前に電子デジタル・コンテンツ・ストア103から認可を受ける。トランザクションID535は、この認証要求の一部としてクリアリング・ハウス105から電子デジタル・コンテンツ・ストア103に渡され、電子デジタル・コンテンツ・ストア103がこの要求をエンドユーザによって実行された先行トランザクションに関連付けることができるようにする。このトランザクションID535は、電子デジタル・コンテンツ・ストア103が使用したいと希望する任意の固有値にすることができ、単にそのストアのためだけのものである。【0300】トランザクション・データ642は顧客名も含む。この名前は、購入を行うときにユーザが記入した購入書式のユーザ名フィールドから得るか、または電子デジタル・コンテンツ・ストア103での何らかのユーザ登録プロセス中に事前にログ記録された情報から得るか、あるいはこのトランザクションで使用したカードに関連するクレジット・カード情報から得た公式名に

することができる。この名前は、後でライセンス・ウォーターマーク527に含まれる。

【0301】トランザクション・データ642は、エンドユーザが購入したストア使用条件519も含む。この情報は、ライセンス・ウォーターマーク527に含まれ、コピー再生制御においてエンドユーザ装置109が使用する。

【0302】トランザクション・プロセッサ・モジュール175が必要とする最終パラメータは、購入決済を確認するHTMLページまたはCGI URLである。その目的は、電子デジタル・コンテンツ・ストア103が金融決済の肯定応答およびその応答に含めたいと希望するその他の情報によってエンドユーザに回答できるようにすることである。このHTMLページまたはCGI URLは、トランザクションSC640に含まれ、トランザクションSC640を受け取って処理したときにエンドユーザ装置109のブラウザ・ウィンドウに表示される。

【0303】トランザクションSC640は、購入提示を処理した後に電子デジタル・コンテンツ・ストア103からエンドユーザに送られるHTTP応答である。直接HTTP応答としてSCを送ると、エンドユーザ装置109へのSCプロセッサ・ヘルパ・アプリケーションの自動ロードが強制的に行われ、その結果、それ以上のエンドユーザ開始アクションに依存せずにトランザクションの自動完了が可能になる。このプロセスについては、以下のエンドユーザ装置109およびブレイヤ・アプリケーション195の項で詳述する。

【0304】必須パラメータを指定してトランザクション・プロセッサ・モジュール175が呼び出されると、このモジュールは、トランザクション・データ642、トランザクション肯定応答HTMLページ、SCのその他の必須セキュリティ機能への参照URLを含むトランザクションSC640を構築し、この購入に関連するオファーSC641を取り出して埋め込む。また、これは、通知インタフェース・モジュール176および会計調停ツール179が後で使用するためにこのトランザクションに関する情報をログ記録する。

【0305】4. 通知インタフェース・モジュール176

通知インタフェース・モジュール176は、ウェブ・サーバ側の実行可能ルーチン(CGIまたはNSAPI、ISAPI、またはこれと同等のものによって呼び出し可能な機能)である。これは、クリアリング・ハウス105、エンドユーザ装置109、コンテンツ・ホスト・サイト111、コンテンツ・プロバイダ101からの任意選択の要求および通知を処理する。電子デジタル・コンテンツ・ストア103が任意選択で通知を要求できるイベントは以下の通りである。

・ エンドユーザ装置109が暗号化キー632を要求

し、クリアリング・ハウス105が指定のコンテンツ113のために暗号化キー623をリリースするというクリアリング・ハウス105からの通知。この通知は任意選択で、暗号化キー623をエンドユーザ装置109に送る前に電子デジタル・コンテンツ・ストア103からの認証を必要とするように構成することができる。

・ コンテンツSC630がエンドユーザ装置109に送られたというコンテンツ・ホスト・サイト111からの通知。

10 ・ コンテンツSC630およびライセンスSC660が受け取られ、コンテンツ113を処理するために正常に使用されたかまたは壊れていることが分かったというエンドユーザ装置109からの通知。

・ 新しいコンテンツ113がコンテンツ・プロモーション・ウェブ・サイト156内に置かれたというコンテンツ・プロバイダ101からの通知。

【0306】これらの通知のいずれも、セキュア・デジタル・コンテンツ電子配布システム100のフローの必須ステップではないが、その販売の完了を満たしたときにそのレコードを閉じる機会を電子デジタル・コンテンツ・ストア103に与えるオプションとして用意されている。また、これは、トランザクションの最終決済以降にどの機能が発生したかまたは販売を完了しようと試みている最中にどのエラーが発生したかを電子デジタル・コンテンツ・ストア103に知らせることにより、顧客サービス要求を処理するために必要になると思われる情報も提供する。あるいは、この状況の多くは、必要に応じて顧客サービス・インタフェース184によりクリアリング・ハウス105から得ることができる。

30 【0307】コンテンツ・プロモーション・ウェブ・サイト156で入手可能な新しいコンテンツ113の通知頻度はコンテンツ・プロバイダ101によって決定される。新しいメタデータSC620が追加されるたびにまたは毎日その日に追加されたすべての新しいメタデータSC620により、通知を行うことができる。

40 【0308】このような通知のいずれでも、結果的にトランザクション・ログ178への入力が行われる。電子デジタル・コンテンツ・ストア103は、このような通知に対してそれ自体の処理を実行したいと希望する場合、CGI呼出しをインターセプトし、固有の機能を実行し、任意選択で通知インタフェース・モジュール176にその要求を渡すことができる。

【0309】5. 会計調停ツール179

この会計調停ツール179は、トランザクション・ログ178とクリアリング・ハウス105のログを比較するようクリアリング・ハウス105に連絡する。これは、セキュア・デジタル・コンテンツ電子配布システム100のための会計処理を快適に行えるように電子デジタル・コンテンツ・ストアを支援するために使用可能な任意選択のプロセスである。

【0310】他の実施形態では、コンテンツ・プロバイダ101およびクリアリング・ハウス105への自動定期支払のために電子資金振替を行えるようにこのツールを更新することができる。また、これは、トランザクション・ログ178と照らし合わせて請求内容を調停した後でクリアリング・ハウス105から電子請求書を受け取り次第、支払を自動的に処理するように設計することもできる。

【0311】C. 同報通信電子デジタル・コンテンツ配布サービス

同報通信とは、主として、オンデマンド視聴をカスタマイズするためにエンドユーザ装置109と電子デジタル・コンテンツ・ストア103との間で個人的対話が一切行われない1対多数の伝送方法を意味する。これは通常、すべてのエンドユーザ装置109が同じストリームを受け取るようにコンテンツ113が事前プログラミングされているデジタル衛星またはケーブル・インフラストラクチャにより提供される。

【0312】サイト設計における多大な共通性により、インターネット接続によるウェブ配布インタフェースならびに同報通信サービスによるより高帯域の衛星またはケーブル配布インタフェースの両方を提供できるように構成されたデジタル・コンテンツ・サービスを電子デジタル・コンテンツ・ストア103が提供するようなハイブリッド・モデルも定義することができる。IRDバック・チャンネル・シリアル・インタフェースがウェブに接続され、IRDがウェブ・ナビゲーションをサポートすれば、エンドユーザはバック・チャンネル・インターネット・インタフェースによる通常のやり方でデジタル・コンテンツ・サービスをナビゲートし、購入するためのコンテンツ113をブライズし選択することができるだろう。ユーザは、いずれもインターネット接続により、高品質のダウンロード可能なコンテンツ113を選択し、このような選択を購入し、必須ライセンスSC660を受け取ることができ、その後、より高帯域の同報通信インタフェースによりコンテンツ113（コンテンツSC630）の送達を要求することができる。ウェブ・サービスは、同報通信スケジュールに基づいてどのコンテンツ113がこのようにダウンロード用に使用可能になるかを示すことができ、あるいは購入したコンテンツ113に完全に基ついて同報通信ストリームを構築できるだろう。この方法により、ウェブ・ベースのデジタル・コンテンツ・サービスは同報通信施設と契約を結び、限られた数の特定のコンテンツ113（たとえば、歌曲またはCD）をこのようにして毎日使用可能にし、カタログ全体をウェブ・インタフェースによるより低品質のダウンロード用に使用可能にする適切な機器を装備したユーザに高品質コンテンツ113を送達することができるだろう。

【0313】エンドユーザ装置109へのウェブ・イン

タフェースが一切存在しないその他の同報通信モデルも設計することができる。このモデルでは、エンドユーザ装置109（すなわち、IRD）に同報通信送達するためにプロモーション・コンテンツが特別にフォーマットしたデジタル・ストリームにパッケージ化され、そこではストリームをデコードし、そこから購入選択を行うことができるプロモーション・コンテンツをエンドユーザに提示するために特別な処理が行われる。

【0314】実際の購入選択は、依然として、エンドユーザ装置109からクリアリング・ハウス105へのバック・チャンネル通信により開始され、SCを使用してすべてのデータ交換を実行することになるだろう。電子デジタル・コンテンツ・ストア103に提供されたツールセットは、そのツールのほとんどがポイントツーポイント・インターネット・サービス・オファリングならびに同報通信衛星またはケーブル・オファリングの両方に適用されるように設計され開発されている。コンテンツ113を取得して管理すると同時にSCを作成するためにデジタル・コンテンツ・ウェブ・サイトの電子デジタル・コンテンツ・ストア103が使用するツールは、同報通信インフラストラクチャ上での配布のためにコンテンツ113を管理し作成するために衛星ベースの電子デジタル・コンテンツ・ストア103も使用する。ウェブ・サービスにより配布されるSCは、同報通信サービスにより配布されるものと同じである。

【0315】1. マルチティア・デジタルTVの実施形態

次に図22に移行すると、本発明により同報通信インフラストラクチャを使用するデジタル・コンテンツの電子配布の代替実施形態を示す高レベル論理図が示されている。この実施形態では、図9で前述したように、コンテンツ・プロバイダ101は1つまたは複数の電子デジタル・コンテンツ・ストア103にメタデータSC620を提供し、1つまたは複数のコンテンツ・ホスト・サイト111にコンテンツSC630を提供する。電子ストア103はメタデータSC620をカスタマイズしてオファーSC641を作成した。オファーSC641は1つまたは複数の同報通信センタ1802に送られる。そのうえ、メタデータSC620に対応するコンテンツSC630は1つまたは複数のコンテンツ・ホスト111から同報通信センタ1802に送られる。オファーSC641は衛星、ケーブル、DirectTV、その他の同報通信メカニズムなどの同報通信インフラストラクチャにより1つまたは複数のエンドユーザ装置109に送られる。この実施形態では、エンドユーザ装置109はテレビのディスプレイ1806とセットトップ・ボックス1804に結合されている。ただし、セットトップ・ボックス1804およびエンドユーザ装置109は論理的かつ物理的に互いに異なる装置または1つの装置にすることができることに留意されたい。エンドユーザ装置1

09は、電話回線などのバック・チャネルによりクリアリング・ハウス105への定期接続を行う。

【0316】図23は、図22の詳細ブロック図であり、本発明により同報通信インフラストラクチャを使用するデジタル・コンテンツの電子配布の代替実施形態を示している。同報通信センタ1802はオフアーSC641を受け取る。カルーセル・ビルダ&ブロードキャスト1902は、同報通信ストリームとともに送られる様々な追加の同報通信コンテンツを作成する。1次同報通信ストリームとともにデジタル情報またはデジタル・コンテンツを伝送するための技法としては、標準のテレビ放送の垂直帰線消去期間に情報を入れるIntelのIntellicastシステムを含む。他の実施形態では、この情報は同報通信伝送用のMP EG-2標準トランスポート・ストリームとして送ることができ、これにより、実質的にすべてのタイプのデジタル同報通信システムによりこのソリューションを配備することができる。図24は、本発明により図22の代替実施形態で同報通信されるバケットのブロック図である。オフアーSC641は、コンテンツSC630およびグローバルSC2040を含む長さNの一連のパッケージ2006に分解され、それはトランザクションSC640と類似しているが、対称キー623に関して重要な相違点がある。グローバルSCの対称キー623は、会計情報を調停するためにエンドユーザ装置109とクリアリング・ハウス105との間で定期接続が行われない場合にコンテンツ113を使用不可にするタイムアウト・メカニズムを有する。対称キー623にタイムアウト設備を設けることにより、エンドユーザ装置109は、まずクリアリング・ハウス105と接続する必要なしに、事前定義期間の間、コンテンツ113を受け取り、アSEMBルし、暗号化解除することができる。期間の1つは、エンドユーザ装置109のユーザの1人が月極定期購読料を支払う加入ベースのサービスにすることができるだろう。ユーザが購読料の支払いとクリアリング・ハウス105との調停を怠った場合、コンテンツ113は使用不可になる。前述のパッケージ2006に加え、コンテンツSC630およびグローバルSC2040と、各コンテンツ113ごとのトラック2002が送られる。音楽の実施形態では、トラック2002は音楽トラックである。パッケージ・フォーマットのカルーセル・フォーマットを図24に示すが、パッケージ2006は循環構造内で同報通信インフラストラクチャにより伝送され、定期的に繰返し現れる。循環同報通信の一部はマスタ・カタログ（図示せず）であり、一連のバケット（P₁... P_N）の一部としてのバグ・カタログはバケット・ストリームの一部として送られる。

【0317】前述のように、デジタル・コンテンツ113はパッケージ2006単位で構成される。1つのパッケージ2006は、プロモーション素材、メタデー

タ、パッケージ記述子、1つの（任意選択の）ビデオクリップに関連付けられている。プロモーション素材はパッケージ・デジタル・コンテンツに関連するグラフィックスおよびテキスト素材からなり（たとえば、音楽アルバムに関連するカバー・アート）、メタデータはそのパッケージに関連する1組の属性値対であり（たとえば、タイトル、価格、アーティストなど）、パッケージ記述子は構造化デジタル・コンテンツをパッケージから抽出するために使用する1組の属性値対であり（たとえば、パッケージサイズおよびセクション数）、ビデオクリップはそのパッケージのコンテンツをビデオ・フォーマットで提示しプロモーションする（たとえば、そのパッケージに関連する音楽アルバムに含まれる歌曲を演奏するアーティストの短い音楽ビデオ）。

【0318】パッケージ2006ならびにプロモーション素材、ビデオクリップ、メタデータ、パッケージ記述子は、カルーセル方式で1つまたは複数のデジタル同報通信チャネルで同報通信センタ1802によって伝送される。カルーセルは、1組の同報通信間隔により繰返し現れる連続デジタル・ストリームである。同報通信受信機により、ユーザはパッケージ2006を選択してダウンロードすると同時にデジタル・コンテンツをパッケージから抽出することができる。

【0319】パッケージ2006は、静的オフアリング（図示せず）と動的オフアリング（図示せず）という2つのセットに構成されている。静的オフアリングはアクティブ・パッケージ2006、すなわち、現在カルーセルで同報通信されているパッケージ2006のセットを表す。動的オフアリングは、サーバ側で使用可能であり、現在同報通信されていないパッケージ2006のセットを表す。次に静的オフアリング・セットは、ビデオクリップ静的オフアリングとビデオカタログ静的オフアリングという2つのサブセットに構成されている。ビデオ・クリップ静的オフアリングはアクティブ・ビデオ・クリップを有するパッケージ2006のセットを表し、ビデオ・カタログ静的オフアリングはアクティブ・ビデオ・クリップを持たないパッケージ2006のセットを表す。

【0320】以下の「X. エンドユーザ装置」の項で詳述するように、セットトップ・ボックス1804上で実行されるアプリケーションは、ビデオ・デコーダ、グラフィカル・ユーザ・インタフェースを提供し、ユーザ入力を受け取る。セットトップ・ボックス1804により、ユーザはデジタルTVチャンネルにチューニングして、ビデオクリップ静的オフアリングに関連するビデオ・クリップを表示することができる。また、セットトップ・ボックス1804により、ユーザは、静的オフアリング・セットと動的オフアリング・セットの両方からダウンロードするためのパッケージ2006を選択することができる。ユーザは、表示された適切なアイコンを選

択することにより、ビデオクリップ静的オフファリング・パッケージ2006を選択してダウンロードし、各パッケージ2006に関連するビデオ・クリップはセットトップ・ボックス1804によって再生される。ユーザは、(1) 静的オフファリング・カタログを表示するアイコン(すなわち、このセットで使用可能なパッケージ2006のアイコン・ベースの図形表現)を選択し、

(2) 所望の選択を突き止めるためにカタログをナビゲートし、(3) 所望のパッケージを選択することにより、ビデオカタログ静的オフファリングを選択してダウンロードする。セットトップ・ボックス1804は同報通信センタ1802と通信して、この動的オフファリング・パッケージの同報通信を要求する。同報通信センタ1802は、ユーザのセットトップ・ボックス1804からすべての要求を収集し、カラーセルにパッケージ2006を割り当て、同報通信間隔にカラーセルを割り当てるスケジューリング・アルゴリズムを実施する。動的オフファリング・パッケージがカラーセルに割り当てられると(したがって、同報通信間隔に割り当てられると)、それは静的オフファリング・パッケージになる。

【0321】すべてのパッケージ2006、プロモーション素材、メタデータ、記述子がマスタ・カタログ内で収集される。マスタ・カタログは事前設定カラーセルで同報通信される。静的オフファリング・セットに属すパッケージ2006はバグ・カタログにリストされる。バグ・カタログは以下のものを含む。

- ・ 静的オフファリング・セットでパッケージを受け取るために必要な同報通信アドレス指定およびチューニング情報
- ・ ビデオ・クリップを受け取るための同報通信アドレス指定情報
- ・ マスタ・カタログを受け取るために必要な同報通信アドレス指定情報
- ・ 現在同報通信されているビデオ・クリップに関連するパッケージを指し示すポインタ
- ・ 静的オフファリング・セットに属すパッケージ2006を表すポインタのセット
- ・ マスタ・カタログ・バージョン
- ・ バグ・カタログ・バージョン

バグ・カタログはポインタのみを含むので、非常に小型であり、頻繁に更新しダウンロードすることができる。このようにして、セットトップ・ボックス1804は同報通信チャンネルの状態によってしきりに更新することができる。

【0322】グラフィカル・ユーザ・インタフェースを構築し表すために、セットトップ・ボックス1804はマスタ・カタログをダウンロードし、含まれるデータを抽出する。選択したパッケージをダウンロードするために、セットトップ・ボックス1804は、そのパッケージを含むカラーセルにチューニングし、そのパッケージ

に関連するデータの収集を開始する。パッケージ・データはセクション単位で構成されている。デジタル伝送エラーにより、セクションは破壊されたり喪失されることがある。セクションの完全性はCRC-32スタイル情報を使用して判定される。一実施形態では、セットトップ・ボックス1804はカラーセル・サイクルによりすべてのパッケージ・セクションを収集する。すべてのセクションが収集され、整理し直されると、セットトップ・ボックス1804はそのパッケージを再アセンブルする。個別の両方向ユニキャスト・チャンネル(インターネットなど)が使用可能である場合、セットトップ・ボックス1804はこのチャンネルを使用して、パッケージの欠落部分を収集することができる。後者のメカニズムを使用すると、パッケージ・ダウンロード時間は大幅に削減される。

【0323】ビデオクリップ静的オフファリング、ビデオカタログ静的オフファリング、動的オフファリング・セットを構築するために、同報通信センタ1802内のストア・マネージャ・アプリケーション(図示せず)を使用する。また、パッケージ2006をカラーセルに関連付け、各カラーセルおよび各ビデオ・クリップの同報通信間隔を決定するためにも、同じアプリケーションを使用する。同報通信マネージャ・アプリケーションによって実行されるアクションは、同報通信センタ1802によってリアルタイムで実施される。

【0324】パッケージ記述子およびプロモーション素材は、受信機のリアルタイム更新を可能にする2ティア・パラダイムを使用して同報通信される。

【0325】2. 個別チャンネルによるウェブ同報通信の実施形態

図31は、図22の詳細ブロック図であり、本発明によりウェブ同報通信サービス内の個別チャンネルを使用するデジタル・コンテンツの電子配布の代替実施形態を示している。図31のこの例示的なアーキテクチャの概要は、同報通信または通信回線による音楽コンテンツの送達のために他の実施形態から加える必要がある少数の変更を例示するために使用したものである。特に、Hughes DirecPCTMなどの現行のウェブキャスト・インフラストラクチャを使用すると、エンドユーザ装置109に関して以下に詳述するように、既存のHughes DirecPCTMシステムとともに機能するように本システムの実施形態のみを適合させるために、トリガ・マネージャ2726など、数個の要素しか追加されない。

【0326】前述のように、同報通信センタ2702は、電子デジタル・コンテンツ・ストア103からオフアーSC641を受け取る。オフアーSC641とともに、対応するコンテンツSC630が取り出される。この実施形態では、オフアーSC641およびコンテンツSC630がコンピュータ記憶装置2704にローカルに記憶される。CGIまたはサーバレット・スクリプ

10

20

30

40

50

ト2708および2710を実行するウェブ・ストア2706は、プロモーション・コンテンツを取得して、図32に示し以下に詳述するようにサンプル・ボタンおよびカタログ・リストを形成する。クレジット・カード、デビット・カード、その他の支払検証システムなどの支払認証を処理するために、eコマースCGI2710は金融クリアリング・ハウス2710とのインタフェースを取る。ウェブ・ストア2706上に置かれたコンテンツはリポジトリ2712に送られる。

【0327】一実施形態では、リポジトリに送られるコンテンツは、バック・チャンネルを介してエンドユーザ装置109から受け取ったユーザ選択に応答するものである。したがって、この実施形態では、エンドユーザ装置109から生じた需要と一致するようにコンテンツをスケジューリングすることができる。そのうえ、より人気のあるユーザ選択がより頻繁に同報通信される場合、リポジトリ2712に送られるコンテンツの周期性を変更することができる。

【0328】オファーSC641およびコンテンツSCは、様々なチャンネル全域で送信機2716による同報通信用を選択される。一実施形態では、サーバ/クローラ2714は、「ウェブ・クローリング」として知られる技法を使用して、伝送すべきコンテンツを取り出すが、その場合、クローラはURLなどの識別子またはその他の何らかの検索プロセスによりコンテンツ参照を自動的にかつ再帰的に取り出す。他の実施形態では、電子デジタル・コンテンツ・ストア103は、オファーSC641およびコンテンツSC630に入れて実施されたコンテンツを「ブッシュ」することができる。コンテンツがアセンブルされると、送信機2716は1つまたは複数の選択チャンネル上でオファーSC641を伝送し、他のチャンネル上で対応するコンテンツSCを伝送する。送信機はDirecPCTMまたは互換性のあるトランシーバである。コンテンツSC630は、個別のダウンロード・チャンネル上でそれぞれ同報通信されるようにパッケージ化することができる。同報通信用の全使用可能通信帯域幅はすべてのチャンネルによって共用される。多数のチャンネルを有する同報通信システムでは、特定のタイトルまたは選択用の各コンテンツSC630は、個別チャンネルで同報通信することができる。このスケジュールは、各チャンネルごとに特定の周期性を保証するように静的に設計することができる。この設計では、非常に人気のあるコンテンツを1つまたは複数のチャンネル上でより頻繁に同報通信することができる。電話回線またはネットワークなどのバック・チャンネルが存在する場合、同報通信コンテンツはユーザ選択に基づいて動的にスケジューリングされる。

【0329】一実施形態では、オファーSC641内のプロモーション素材は、SCから取り出され、チャンネルにより伝送される。プロモーション素材をSC内に保持

する必要性は、そのプロモーション素材によって決まる。

【0330】エンドユーザ装置109は、受信機1804により同報通信を受信する。直接同報通信実施形態の受信機2718は、DirecPCTM用パラボラアンテナまたはDirecPCTM/DirectTVTM兼用パラボラアンテナあるいはそれと同等のウェブ・キャスト同報通信システムに結合されたUSBモデムである。キャッシュ・マネージャ2720は、エンドユーザ装置109でのコンテンツおよびプロモーション素材のダウンロードを管理するソフトウェア・プログラムである。プロモ・キャッシュ2722およびアルバム+DSCバッファ2724という2つのリポジトリが示されている。これらは、エンドユーザ装置109内の2つの別々の記憶領域として示されているが、これらのリポジトリ2722および2724をより多くの記憶領域にさらに分割するか、エンドユーザ装置上の単一記憶領域に結合することができることは当業者には明白になるだろう。しかも、エンドユーザ装置109内の多くのコンポーネントは、1つのユニットに結合するか、受信機2718、キャッシュ・マネージャ2720、ウェブ・ブラウザ191、プロモ・キャッシュ2722、アルバム+DSCバッファ2724を含む個別ハードウェアとして実現することができる。たとえば、一実施形態のDirecPCTMはセットトップ・ボックス1804に収容される。

【0331】DSCという用語の使い方に留意することは重要である。DSCは、「切断SC」の省略形である。これはコンテンツSC630と同一であるが、接頭部「D」はこの実施形態では、エンドユーザ装置が切断されたとき、すなわち、送信機2716から同報通信を受信していないか、バック・チャンネルによりウェブ・ストア2706に返信していないか、あるいはその両方の場合でも、エンドユーザ装置109上でローカルにコンテンツDSCを取り出すことができることを強調するために使用している。

【0332】前述のように、プロモ・キャッシュ2722はエンドユーザ装置109が受信したプロモーションを記憶し、同様にアルバム+DSC2724はコンテンツSC641を記憶する。プロモーション・チャンネルに加入しているユーザの場合、プロモ・キャッシュ2722に記憶されたプロモーション素材またはオファーSC641は、プロモーション・パッケージの新バージョンが同報通信されたときに必ず更新される。プロモーション・コンテンツを最新の状態に保持することにより、ユーザは、オフラインでブラウズしているときにプロモーション・コンテンツが最も最新のものになるよう保証される。より大型のアルバム+DSCバッファ2724を備えたシステムでは、プロモーション素材が更新されたときに、対応するコンテンツSC630が記憶され更新される。コンテンツに関する両方のプロモーション素材

をローカルに記憶すると、コンテンツを含むユーザ・システムが最新のものになる。

【0333】ウェブ・ブラウザ191を使用するユーザは、プロモ・キャッシュ2722に事前にキャッシュされたプロモーション素材をブラウズする。例示的なユーザ・インタフェースは、以下の図32に示されている。前述のようにプロモーション素材が記憶されているので、同報通信センタ2702から同報通信を受信するように「接続」されているか否かにかかわらず、ユーザがプロモーション素材をブラウズできることは留意すべき重要なことである。

【0334】一実施形態では、ユーザがプロモーション素材を選択すると、トリガ・マネージャ2726によって起動されるプレーヤ・アプリケーション196によりサンプル・クリップを再生することができる。ユーザがウェブ・ブラウザ191を使用して選択を行うと、キャッシュ・マネージャは、対応するコンテンツSC630がアルバム+DSCバッファ2724内で使用可能になっているかどうかを確認するためのチェックを行い、対応するコンテンツSC630がすでにダウンロードされている場合、それはキャッシュ・マネージャに与えられ、トリガ・マネージャ2726を起動し、「接続」実施形態のプレーヤ・アプリケーション195に関して前述したようにコンテンツSC630の処理を開始する。対応するコンテンツSC630がアルバム+DSCバッファ2724で使用可能になっていない場合、キャッシュ・マネージャ2720は要求を行う。キャッシュ・マネージャ2720に対する要求または加入要求は、コンテンツSC630の同報通信用に適切なチャネルを選択するよう受信機を制御する。コンテンツSC630用のチャンネルは、ダウンロードするプロモーションごとにプロモ・キャッシュ2722内の1つのテーブルに記憶することができる。このため、同報通信スケジュールの変更をローカルで追跡することができる。コンテンツSC630の次のスケジュール同報通信は、受信機2718によって受信され、アルバム+DSCバッファ2724にローカルにキャッシュされる。キャッシュ・マネージャ2720は、正しい間隔で自動的にウェイクアップしてダウンロードのために対応するチャネルを選択するようにプログラミングすることができる。

【0335】任意選択の実施形態では、同報通信センタ2702へのインターネットなどのバック・チャネルを使用してユーザが次にサインオンまたはログオンすると、eコマース・サイト2710を使用してクレジット・カード支払などのユーザ会計情報の確認が行われる。その他の実施形態では、クリアリング・ハウス105またはウェブ・ストア2706に再接続することなしにユーザが所与の数の購入を行えるようにすることにより、コンテンツ113の「オフライン」購入が実施される。この「オフライン」実施形態では、所与の期間または価

値据置き範囲内で再接続が行われるまで、クレジット限界、購入限界、定期接続、コンテンツ113の時限使用などのいくつかのカテゴリを使用することができる。

【0336】要求された適切なコンテンツSC630のスケジューリングおよびダウンロードをキャッシュ・マネージャ2720が完了すると、トリガ・マネージャ・アプリケーション2726はプレーヤ・アプリケーション195に通知し、コンテンツはアルバム+DSCバッファ2724からプレーヤ・アプリケーション195へのインポートに使用可能になる。コンテンツSCがダウンロードされたことをプレーヤ・アプリケーションに通知することに加え、ダウンロードの状況、ダウンロード時のエラー、所望のコンテンツ113を演奏または再生したいと希望する際にユーザにとって有用なその他の情報などのその他の状況をキャッシュ・マネージャ2720からプレーヤ・アプリケーション195に報告することができる。

【0337】現行の送達システムの「オンライン」または「接続」バージョンについて前述したように、コンテンツに関連する使用条件および権利を更新するために必要なステップはクリアリング・ハウス105によって監視することができる。

【0338】X. エンドユーザ装置109
セキュア・デジタル・コンテンツ電子配布システム100用のエンドユーザ装置109におけるアプリケーションは、第1にSCの処理およびコピー制御と、第2に暗号化コンテンツ113の再生という2つの主な機能を果たす。エンドユーザ装置109は、パーソナル・コンピュータであるか専用の電子消費者装置であるかにかかわらず、これらの基本機能を実行できなければならない。また、エンドユーザ装置109は、再生リストの作成、デジタル・コンテンツ・ライブラリの管理、コンテンツ再生中の情報および画像の表示、外部媒体装置への記録のような様々な追加機構および機能も提供する。このような機能は、これらのアプリケーションがサポートするサービスと、これらのアプリケーションの設計対象である装置のタイプに基づいて様々である。

【0339】A. 概要

次に図13を参照すると、主要コンポーネントおよびプロセスと、エンドユーザ装置109の機能フローが示されている。PCベースのウェブ・インタフェース・コンテンツ113のサービスをサポートするように設計されたアプリケーションは、SCプロセッサ192とプレーヤ・アプリケーション195という2通りの実行可能ソフトウェア・アプリケーションからなる。SCプロセッサ192は、SCファイル/MIMEタイプを処理するためにエンドユーザのウェブ・ブラウザ191内にヘルパ・アプリケーションとして構成された実行可能アプリケーションである。このアプリケーションは、電子デジタル・コンテンツ・ストア103、クリアリング・ハ

ウス105、コンテンツ・ホスト・サイト111からSCを受け取ったときに必ずブラウザによって立ち上げられる。これは、SCに関するすべての必須処理を実行し、最終的にコンテンツ113をエンドユーザのデジタル・コンテンツ・ライブラリ196に追加することを担当する。

【0340】プレーヤ・アプリケーション195は、自分のデジタル・コンテンツ・ライブラリ196内のコンテンツ113を実行し、自分のデジタル・コンテンツ・ライブラリ196を管理し、許されるならばコンテンツ113のコピーを作成するためにエンドユーザがロードするスタンドアロンの実行可能アプリケーションである。プレーヤ・アプリケーション195とSCプロセッサ192の両方のアプリケーションは、Java、C/C++、またはそれと同等のソフトウェアで作成することができる。好ましい実施形態では、ウェブサイトなどのコンピュータ可読手段からアプリケーションをダウンロードすることができる。しかし、ディスクまたはCDなどのコンピュータ可読手段で送達するなど、その他の送達メカニズムも可能である。

【0341】コンテンツ113の情報のサーチおよびブラウズ、たとえば歌曲クリップのレビュー、購入用の歌曲の選択は、いずれもエンドユーザのウェブ・ブラウザ191により処理される。電子デジタル・コンテンツ・ストア103は、多くのコンテンツ113小売ウェブ・サイトにより今日提供されるものと同じ方法でショッピング経験を提供するものである。エンドユーザにとって今日のウェブ・ベースのコンテンツ113ショッピングを上回る相違点は、自分のショッピング・カートに追加すべきダウンロード可能なコンテンツ113のオブジェクトを選択できることである。電子デジタル・コンテンツ・ストア103がダウンロード可能なオブジェクトに加え販売用に使用可能なその他の商品を有する場合、エンドユーザは自分のショッピング・カート内に物理的商品とダウンロード可能な電子商品との組合せを有することができる。エンドユーザがチェックし、自分の最終購入許可を電子デジタル・コンテンツ・ストア103に提示するまで、セキュア・デジタル・コンテンツ電子配布のエンドユーザ装置109は関わりがない。この時点の前のすべての対話は、電子デジタル・コンテンツ・ストア103用のウェブ・サーバとエンドユーザ装置109上のブラウザ191との間で行われる。これは、サンプル・デジタル・コンテンツ・クリップのレビューを含む。デジタル・コンテンツ・クリップはSC内にパッケージ化されないが、むしろ、ダウンロード可能なファイルとして電子デジタル・コンテンツ・ストア103のウェブ・サービスに統合されるかまたはストリーミング・サーバから供給される。コンテンツ113クリップのフォーマットはシステム・アーキテクチャによって指示されない。他の実施形態では、プレー

ヤ・アプリケーション195が電子デジタル・コンテンツ・ストア103またはクリアリング・ハウス105と直接対話するか、あるいはプロモーションCDを使用してオフラインで対話することができるだろう。

【0342】B、アプリケーションのインストールプレーヤ・アプリケーション195とヘルパ・アプリケーション198は、多くのウェブ・サイトからダウンロード用に使用可能な自己インストール実行可能プログラムにパッケージ化される。クリアリング・ハウス105は、パブリック・ウェブ・サイトにあるマスタ・ダウンロード・ページのホストとなる中央位置として動作する。これは、そこからインストール・パッケージをダウンロードすることができる位置へのリンクを含む。このインストール・パッケージは、ダウンロード要求の地理的分散を可能にするためにすべてのコンテンツ・ホスト・サイト111で入手可能である。各参加電子デジタル・コンテンツ・ストア103もそのサイトからのダウンロード用にそのパッケージを使用可能な状態にすることができる場合もあれば、クリアリング・ハウス105のパブリック・ウェブ・サイトにあるマスタ・ダウンロード・ページへのリンクを提供するだけの場合もある。

【0343】ダウンロード可能なコンテンツ113を購入したいと希望するエンドユーザは、このパッケージをダウンロードしてインストールする。このインストールは、このダウンロード可能なパッケージ内で独立したものである。これは、ヘルパ・アプリケーション198とプレーヤ・アプリケーション195の両方をアンパックしてインストールし、インストールされたウェブ・ブラウザに依拠してヘルパ・アプリケーション198の構成も行う。

【0344】インストールの一部として、オーダおよびライセンスSC660を処理する際に使用するためにエンドユーザ装置109用に公開/秘密キー661の対が作成される。ライセンス・データベース197内の歌曲暗号化キーを保護する際に使用するためにランダム対称キー（機密ユーザ・キー）も生成される。この機密ユーザ・キー（図示せず）は、そのキーを複数のパーツに分解し、そのキーのピースをエンドユーザのコンピュータ全体の複数の位置に記憶することによって保護される。このコードの領域は、そのキーがどのようにセグメント化され、どこに記憶されているかを漏らさないように改竄防止ソフトウェア技術によって保護される。エンドユーザによるこのキーへのアクセスすら防止することにより、その他のコンピュータとのコンテンツ113の共用または著作権侵害を防止するのに役に立つ。これらのキーの使い方の詳細についてはSCプロセッサ192の項を参照されたい。

【0345】改竄防止ソフトウェア技術は、ハッカによるコンピュータ・ソフトウェア・アプリケーションへの無許可侵入を阻止するための方法である。通常、ハッカ

はソフトウェアを理解したいと希望するか、ソフトウェアを変更してその使用に関する制限を除去したいと希望するものである。特に、侵入できないコンピュータ・プログラムはまったく存在せず、これが改竄防止ソフトウェアが「耐改竄性」と呼ばれない理由である。しかし、改竄防止保護アプリケーションに侵入するのに必要な労力は得られる利益に値しないので、通常、ほとんどのハッカを阻止することになる。この場合、その労力はコンテンツ113の1つのピース、おそらくCD上の1つの歌曲へのキーにアクセスすることになるだろう。

【0346】1つのタイプの改竄防止ソフトウェア技術はIBMから得られる。このコードが導入された製品の1つは、IBMのThinkPad770ラップトップ・コンピュータに内蔵されている。この場合、改竄防止ソフトウェアはコンピュータ内のDVD映画プレーヤを保護するために使用された。ハリウッド・スタジオなどのデジタル・コンテンツ・プロバイダは、デジタル映画の出現と完璧なコピーを作成できる容易さを懸念し、DVDディスク上の映画がコピー保護メカニズムを含むべきだと主張してきた。IBMの改竄防止ソフトウェアは、この

ようなコピー保護メカニズムを回避しにくくするものである。これは改竄防止ソフトウェアにとって非常に典型的な応用例であり、このソフトウェアを使用して、何らかの保護タイプのコンテンツ113の使用に関する規則を施行する。

【0347】IBMの改竄防止ソフトウェアは、攻撃者の経路にいくつかのタイプの障害物を置くものである。第1に、それはハッカが使用する標準的なソフトウェア・ツール、すなわち、デバッグおよび逆アセンブラを無効にするかまたは少なくともその効力を低減するための技法を含む。第2に、それは自己完全性チェックを含むので、単一変更またはほんの少数の変更でも検出され、間違った動作を引き起こすことになる。最後に、それは、その本当の動作に関してハッカを誤解させるための不明化部分を含む。後者の技法は主として特定の問題のみに関するものであるが、最初の2つは暗号化およびデジタル・シグニチャという暗号化技術で周知のツールに基づくものである。

【0348】C. セキュア・コンテナ・プロセッサ192
エンドユーザが自分のショッピング・カートに収集した商品について電子デジタル・コンテンツ・ストア103に最終購入許可を提示すると、そのウェブ・ブラウザは、ウェブ・サーバからの応答を待ってアクティブなまになる。電子デジタル・コンテンツ・ストア103のウェブ・サーバは、その購入を処理し、金融決済を実行し、トランザクションSC640をエンドユーザ装置109に返す。トランザクションSC640に関連するSCMIMEタイプを処理するために、ウェブ・ブラウザによってSCプロセッサ192（ヘルバ・アプリケー

ション198）が立ち上げられる。図17は、本発明により図13に記載するようにローカル・ライブラリにコンテンツをダウンロードするプレーヤ・アプリケーション195のユーザ・インタフェース画面の一例である。

【0349】SCプロセッサ192は、トランザクションSC640をオープンし、そこに含まれるオファースC641と応答HTMLページを抽出する。応答HTMLページはエンドユーザの購入を確認するブラウザ・ウィンドウに表示される。次にステップ1401でオファースC641がオープンされ、予定ダウンロード時間とともにコンテンツ113（たとえば、歌曲またはアルバム）の名前がそこから抽出される。次にステップ1402でこの情報を含む新しいウィンドウが表示され、コンテンツ113のダウンロードをスケジューリングするためのオプション（たとえば、音楽の場合は複数歌曲またはアルバム全体）がエンドユーザに提示される。エンドユーザは即時ダウンロードを選択するかまたはダウンロードを後で行うようにスケジューリングすることができる。後で行うことを選択した場合、ダウンロード・スケジューリング情報がログに保管され、エンドユーザ装置109がその予定時間に電源投入された場合にその時点でダウンロードが開始される。その予定ダウンロード時間にコンピュータがアクティブになっていないかまたは通信リンクがアクティブになっていない場合、エンドユーザは、コンピュータが次に電源投入されたときにダウンロードのスケジューリングをやり直すよう要求される。

【0350】予定ダウンロード時間が発生するかまたは即時ダウンロードが要求された場合、SCプロセッサ192は、トランザクションSC640、オファースC641、インストール時に作成されたエンドユーザの公開キー661内の情報からオーダSC650を作成する。このオーダSC650はHTTP要求によりクリアリング・ハウス105に送られる。クリアリング・ハウス105がライセンスSC660を返すと、ライセンスSC660を処理するためにヘルバ・アプリケーション198が再呼出しされる。次にライセンスSC660がオープンされ、参照したオーダSC650からコンテンツ・ホスト・サイト111のURLが抽出される。次にコンテンツSC630のダウンロードを要求するブラウザによるhttp要求によって、ライセンスSC660が指定のコンテンツ・ホスト・サイト111に送られる。コンテンツSC630がブラウザに戻ると、ヘルバ・アプリケーション198がもう一度、再呼出しされる。SCプロセッサ192は、ダウンロード経過インジケータおよび推定完了時間とともにダウンロード中のコンテンツ113の名前を表示する。

【0351】SCプロセッサ192によってコンテンツ113が受信されると、それは暗号化解除のためにコンテンツ113のデータをメモリ・バッファにロードする。バッファのサイズは、暗号化アルゴリズムとウォー

10

20

30

40

50

タマーク技術193の要件によって決まり、ハッカ・コードに曝される未暗号化コンテンツ113の量を低減するために可能な最小サイズになっている。バッファがいっぱいになると、それはライセンスSC660から抽出したエンドユーザのキー623（公開キー661に対応するもの）を使用して暗号化解除されるが、それ自体はまず秘密キーを使用して暗号化解除される。次に、暗号化解除したバッファがウォーターマーク機能に渡される。

【0352】ウォーターマーク193は、ライセンスSC660からウォーターマーク命令を抽出し、エンドユーザの秘密キーを使用してその命令を暗号化解除する。次にウォーターマーク・データは、そこからこのコンテンツ113が購入された電子デジタル・コンテンツ・ストア103に登録された購入者の名前などのトランザクション情報を含むライセンスSC660から抽出されるか、あるいは電子デジタル・コンテンツ・ストア103が登録機能を提供しない場合はクレジット・カード登録情報から導出される。また、ウォーターマークには、購入日と、このトランザクションに関してログ記録された特定のレコードを参照するために電子デジタル・コンテンツ・ストア103が割り当てたトランザクションID535も含まれる。また、プレーヤ・アプリケーション195のコピー制御が使用するためにストア使用条件519も含まれる。

【0353】ウォーターマーク193は、ウォーターマーク命令を漏らさないように改竄防止コード技術によって保護され、したがって、ハッカがウォーターマークの位置および技法を発見するのを防止する。これにより、ハッカによるウォーターマークの除去または変更が防止される。

【0354】このコンテンツ・バッファに必須ウォーターマークを銘記した後、そのバッファは再暗号化194用のスクランブル機能に渡される。IBMのSEAL暗号化技術などのプロセッサ有効セキュア暗号化アルゴリズムを使用して、ランダム対称キーによりコンテンツ113を再暗号化する。ダウンロード、暗号化解除、再暗号化194のプロセスが完了すると、本来コンテンツ113を暗号化するためにコンテンツ・プロバイダ101が使用した暗号化キー623はこの時点で破壊され、インストール時に作成され隠された機密ユーザ・キーを使用して新しいSEALキー自体が暗号化される。次にこの新しい暗号化SEALキーはライセンス・データベース107に記憶される。

【0355】コンテンツ・プロバイダ101側で実行される異なるソース、および、エンドユーザ装置109側で実行されるユーザ・ウォーターマークは、効果的であるために業界標準になる必要があるであろう。このような標準は依然として進化している。この技術は、制御信号を音楽に埋め込み、何回も更新できるようにするために使用可能なものである。コピー制御標準がより安定したものになる時点まで、セキュア・デジタル・コンテン

ツ電子配布システム100には代替コピー制御方法が設けられていたので、消費者装置内で権利管理を可能にするためにコピー制御ウォーターマークをあてにしない。記憶および再生/記録使用条件のセキュリティは、エンドユーザ装置109に結合された暗号化DCライブラリ・コレクション196を使用して実現され、改竄防止環境によって保護される。ソフトウェア・フックは、標準が採用されたときにコピー制御ウォーターマークをサポートするために所定の位置にある。現在、様々な圧縮レベルでのウォーターマークAAAおよびその他のコード化オーディオ・ストリームのサポートが存在するが、この技術はコピー制御の単独方法として利用するにはこの時点では依然としていくらか時期尚早である。

【0356】暗号化解除および再暗号化194のプロセスは、元のコンテンツ113の暗号化キー、新しいSEALキー、機密ユーザ・キー、機密ユーザ・キーのセグメントがどこに記憶されるか、そのキーがどのようにセグメント化されるかを漏らさないように改竄防止コード技術によって保護される、もう1つのコード領域である。

【0357】暗号化解除および再暗号化194のプロセスは2つの目的に対応する。SEALのようなアルゴリズムによって暗号化されたコンテンツ113を記憶するとリアルタイム暗号化解除より高速になり、DESのようにより業界標準タイプのアルゴリズムを実行する場合より暗号化解除を実行するのに必要なプロセッサ使用率がかなり低下する。これにより、プレーヤ・アプリケーション195は、デコードおよび再生の前にコンテンツ113用のファイル全体を先に暗号化解除する必要なしに、コンテンツ113のリアルタイム同時暗号化解除デコード再生を実行することができる。SEALアルゴリズムおよび非常に効率の良いデコード・アルゴリズムの効率により、同時動作（暗号化ファイルからのストリーミング再生）が可能になるだけでなく、かなり低電力のシステム・プロセッサ上でこのプロセスを行うこともできる。したがって、このアプリケーションは、60MHzのPentiumシステムおよびそれ以下程度のローエンドのエンドユーザ装置109上でサポートすることができる。コンテンツ113が最終的に記憶される暗号化フォーマットを元の暗号化フォーマットから分離すると、元のコンテンツ暗号化アルゴリズムの選択の際に柔軟性の増大が可能になる。したがって、広く受け入れられ立証された業界標準アルゴリズムを使用することができ、その結果、デジタル・コンテンツ業界によるセキュア・デジタル・コンテンツ電子配布システム100の容認がさらに強化される。

【0358】この暗号化解除および再暗号化194のプロセスの第2の目的は、このコンテンツ113を暗号化するためにコンテンツ・プロバイダ101が使用した元のマスタ暗号化キー623はこのコンテンツ113のラ

ライセンスを許諾したすべてのエンドユーザ装置109上に記憶しなければならないという要件を除去することである。ライセンスSC660の一部としての暗号化マスターキー623は、非常に短時間の間、エンドユーザ装置109のハード・ディスク上にキャッシュされるだけであり、メモリ内でのみ非常に短時間の間、平文になる。この実行フェーズ中、キー623は改竄防止コード技術により保護される。この暗号化解除および再暗号化194のフェーズが完了すると、エンドユーザ装置109上でいずれかの形式でこのキー623を保持する必要はなくなるので、ハッカによる著作権侵害の可能性は大幅に軽減される。

【0359】歌曲は、再暗号化されると、デジタル・コンテンツ・ライブラリ196に記憶される。プレーヤ・アプリケーション195が使用するために必要なすべてのメタデータは関連オフターSC641から抽出され、ステップ1403でデジタル・コンテンツ・ライブラリ196にも記憶される。歌曲の歌詞など、暗号化されたメタデータのいずれかの部分は、他のコンテンツに関して前述したのと同じように暗号化解除され再暗号化される。暗号化が必要な関連メタデータには、コンテンツ113を暗号化するために使用したのと同じSEALキーを使用する。

【0360】D. プレーヤ・アプリケーション195

1. 概要

セキュア・デジタル・コンテンツ電子配布プレーヤ・アプリケーション195（ここではプレーヤ・アプリケーション195という）は、CD、DVD、その他のデジタル・コンテンツ・プレーヤと、CD、DVD、その他のデジタル・コンテンツ記憶管理システムの両方に類似したものである。これは、その最も単純なレベルでは、歌曲またはビデオの再生など、コンテンツ113を実行する。他のレベルでは、自分のデジタル・コンテンツ・ライブラリ196を管理するためのツールをエンドユーザに提供する。まさに重要なことに、歌曲などのコンテンツのコレクション（ここでは再生リストという）の編集および再生を可能にする。

【0361】プレーヤ・アプリケーション195は、個々に選択し、コンテンツ・プロバイダ101および電子デジタル・コンテンツ・ストア103の要件に応じてカスタマイズ可能なコンポーネントの集合からアセンブルされる。このプレーヤの汎用バージョンについて説明するが、カスタマイズは可能である。

【0362】次に図18および図19を参照すると、図13のエンドユーザ装置109上で実行されるプレーヤ・アプリケーション195の主要コンポーネントおよびプロセスのブロック図が示されている。

【0363】プレーヤ・オブジェクト・マネージャ1501のサブシステムを構成するコンポーネントセットがいくつか存在する。

1. エンドユーザ・インタフェース・コンポーネント1509
 2. コピー/再生管理コンポーネント1504
 3. 暗号化解除1505、圧縮解除1506、再生1507の各コンポーネント、記録を含むことができる
 4. データ管理1502およびライブラリ・アクセス1503の各コンポーネント
 5. アプリケーション間通信コンポーネント1508
 6. その他の各種（インストールなど）コンポーネント
- 【0364】これらの各セット内から以下の要件に基づいてコンポーネントを選択することができる。

- ・ プラットフォーム（Windows（登録商標）、UNIX（登録商標）、それと同等のもの）
- ・ 通信プロトコル（ネットワーク、ケーブルなど）
- ・ コンテンツ・プロバイダ101または電子デジタル・コンテンツ・ストア103
- ・ ハードウェア（CD、DVDなど）
- ・ クリアリング・ハウス105の技術など

【0365】以下の各項は様々なコンポーネント・セットを詳述するものである。最終項では、これらのコンポーネントがどのように汎用プレーヤに編成されるかを詳述し、そのコンポーネントをどのようにカスタマイズできるかを説明する。

【0366】他の実施形態では、プレーヤ・アプリケーション195およびSCプロセッサ192のコンポーネントがプログラマのソフトウェア・ツールキットの一部として使用可能になる。このツールキットは、上記の汎用プレーヤ・アプリケーションの各種コンポーネントへの事前定義インタフェースを可能にする。このような事前定義インタフェースは、APIまたはアプリケーション・プログラミング・インタフェースの形になっている。このようなAPIを使用する開発者は、各種コンポーネントの機能性のいずれについても高レベル・アプリケーション・プログラムから実現することができる。このようなコンポーネントにAPIを提供することにより、プログラマは、このようなコンポーネントのいずれのについてもその機能およびリソースを再作成する必要なしに、カスタマイズしたプレーヤ・アプリケーション195を迅速に開発することができる。

【0367】2. エンドユーザ・インタフェース・コンポーネント1509

このセットからのコンポーネント同士が協力し、プレーヤ・アプリケーション195の画面上での発現を可能にする。ただし、設計ではこれらのコンポーネントの決定的なレイアウトを設定していないことに留意されたい。このようなレイアウトの1つは汎用プレーヤに設けられている。コンテンツ・プロバイダ101または電子デジタル・コンテンツ・ストアあるいはその両方からの要件ならびにその他の要件に基づいて、代替レイアウトも可能である。

【0368】このセットは、エンドユーザ表示1510を提示し、オーディオ再生およびメタデータの提示などの低レベル機能に使用するエンドユーザ・コントロール1511というコントロールを扱うために使用するコンポーネントから始まって、複数のサブグループにグループ化される。次にエンドユーザ表示コンポーネント1510は特殊機能のグループ化（再生リスト、デジタル・コンテンツ・ライブラリ）によってさらに分割され、次にオブジェクトコンテナ・コンポーネントはこのような低レベル・コンポーネントのグループ化および配置に使用する。

【0369】以下のコンポーネント・リスト内では、CDの作成あるいはCDまたはその他の記録可能媒体へのコンテンツ113のコピーについて言及した場合、それはプレーヤ・アプリケーション195がこのような機能性を使用可能にした場合にのみ適用される。また、その文脈で使用するCDという用語は汎用のものであり、ミニディスクまたはDVDなど、その他の様々な記録装置も表すことができることに留意されたい。

【0370】図20は、本発明により図18ないし図19のプレーヤ・アプリケーション195のユーザ・インタフェース画面の一例である。エンドユーザ・コントロール1511用の機能としては以下のものを含む（エンドユーザ・インタフェースの対応画面を1601～1605として示す）。

コンテンツ113を実行するためのコントロール：

- ・ 再生/停止ボタン
- ・ 再生ボタン
- ・ 停止ボタン
- ・ 休止ボタン
- ・ 前進スキップ・ボタン
- ・ 後退スキップ・ボタン
- ・ ボリューム・コントロール
- ・ トラック位置コントロール/表示
- ・ オーディオ・チャンネル・ボリューム・レベル表示など

コンテンツ113に関連するメタデータを表示するためのコントロール

- ・ カバー・ピクチャ・ボタン
- ・ カバー・ピクチャ・オブジェクト
- ・ アーティスト・ピクチャ・ボタン
- ・ アーティスト・ピクチャ・オブジェクト
- ・ トラック・リスト・ボタン
- ・ トラック・リスト情報オブジェクト
- ・ トラック・リスト・セレクト・オブジェクト（クリックして再生）
- ・ トラック名オブジェクト
- ・ トラック情報オブジェクト
- ・ トラック歌詞ボタン
- ・ トラック歌詞オブジェクト

- ・ トラック・アーティスト名オブジェクト
- ・ トラック・クレジット・ボタン
- ・ トラック・クレジット・オブジェクト
- ・ CD名オブジェクト
- ・ CDクレジット・ボタン
- ・ CDクレジット・オブジェクト
- ・ 汎用（構成可能）メタデータ・ボタン
- ・ 汎用メタデータ・オブジェクトなど

【0371】エンドユーザ表示1510用の機能としては以下のものを含む（エンドユーザ・インタフェースの対応画面を1601～1605として示す）。

表示コンテナの再生リスト

- ・ 再生リスト管理ボタン
- ・ 再生リスト管理ウィンドウ
- ・ デジタル・コンテンツ・サーチ・ボタン
- ・ デジタル・コンテンツ・サーチ定義オブジェクト
- ・ デジタル・コンテンツ・サーチ提示ボタン
- ・ デジタル・コンテンツ・サーチ結果オブジェクト
- ・ 再生リストへの選択サーチ結果項目コピー・ボタン
- ・ 再生リスト・オブジェクト（編集可能）
- ・ 再生リスト保管ボタン
- ・ 再生リスト再生ボタン
- ・ 再生リスト休止ボタン
- ・ 再生リスト再始動ボタン
- ・ 再生リストからのCD作成ボタンなどデジタル・コンテンツ・ライブラリ196の表示

- ・ デジタル・コンテンツ・ライブラリ・ボタン
- ・ デジタル・コンテンツ・ライブラリ・ウィンドウ
- ・ デジタル・コンテンツ・カテゴリ・ボタン
- ・ デジタル・コンテンツ・カテゴリ・オブジェクト
- ・ アーティスト別ボタン
- ・ ジャンル別ボタン
- ・ レーベル別ボタン
- ・ カテゴリ別ボタン
- ・ 削除ボタン
- ・ 再生リストへの追加ボタン
- ・ CDへのコピー・ボタン
- ・ 歌曲リスト・オブジェクト
- ・ 歌曲リスト表示コンテナなど

40 コンテナおよびその他

- ・ プレーヤ・ウィンドウ・コンテナ
- ・ オーディオ・コントロール・コンテナ
- ・ メタデータ・コントロール・コンテナ
- ・ メタデータ表示コンテナ
- ・ ツールバー・コンテナ・オブジェクト
- ・ サンプル・ボタン
- ・ ダウンロード・ボタン
- ・ 購入ボタン
- ・ 記録ボタン

50 プレーヤ名オブジェクト

- ・ レーベル/プロバイダ/ストア広告オブジェクト
- ・ レーベル/プロバイダ/ストアURLボタン
- ・ アーティストURLボタンなど

【0372】3. コピー/再生管理コンポーネント1504

これらのコンポーネントは、暗号化キーのセットアップ、ウォーターマーク処理、コピー管理などを処理する。また、クリアリング・ハウス105との通信、購入要求の伝送などのため、ペイパーリッスンなどの特殊サービスまたはコンテンツ113にアクセスすることに課金する場合のためのインタフェースも存在する。現在、クリアリング・ハウス105の諸機能への通信はSCプロセッサ192によって処理されている。

【0373】エンドユーザ装置109上のプレーヤ・アプリケーション195によるコンテンツ113の使用は、ライセンス・データベース197などのデータベースにログ記録される。プレーヤ・アプリケーション195によるコンテンツ113の使用ごとの追跡は、クリアリング・ハウス105またはコンテンツ・プロバイダ101または電子デジタル・コンテンツ・ストア103または指定され伝送インフラストラクチャ107に結合された任意のサイトなどの1つまたは複数のログ記録サイトに伝送することができる。この伝送は、ログ記録サイトに使用情報をアップロードするために所定の時間にスケジューリングすることができる。企図する所定の時間の1つは、伝送インフラストラクチャ107がネットワーク・トラフィックで混雑しないと思われる早朝である。既知の技法を使用するプレーヤ・アプリケーション195は、計画した時間にウェイクアップし、ローカル・ログ記録データベースからそのログ記録サイトに情報を伝送する。ログ記録サイト情報を検討することにより、コンテンツ・プロバイダ101はそのコンテンツ113の人気を測ることができる。

【0374】他の実施形態では、ログ記録サイトに後でアップロードするためにコンテンツ113の使用をログ記録する代わりに、コンテンツ113の使用中に必ずコンテンツ113の使用をログ記録サイトにアップロードする。たとえば、エンドユーザ装置109に記憶したコンテンツ113をDVDディスク、デジタル・テープ、フラッシュ・メモリ、ミニディスク、またはそれと同等の読取り/書き込み可能取外し可能媒体などの外部装置上に複製またはコピーする場合、その使用はログ記録サイトにアップロードされる。これは、コンテンツ113を購入したときに伝送される使用条件206において、コンテンツ113をコピーするための前提条件になる可能性がある。これは、コンテンツ・プロバイダ101がコンテンツ113に対して自分が再生、複製、その他のアクションを行っている最中に自分のコンテンツ113の使用を正確に追跡できることを保証するものである。

【0375】そのうえ、コンテンツ113に関するその他の情報をログ記録サイトにアップロードすることができる。たとえば、コンテンツ113を最後に実行した時間（たとえば、時間および日付）、コンテンツ113を何回実行したか、DVDディスク、デジタル・テープ、ミニディスクなどの許可された外部装置にコンテンツ113を複製またはコピーした場合などである。エンドユーザ装置109上の単一プレーヤ・アプリケーション195について、1所帯内の各種家族など、複数の別個のユーザが存在する場合、コンテンツ113のユーザの識別名は使用情報とともにログ記録サイトに伝送される。ログ記録サイトにアップロードされた使用情報を検討することにより、コンテンツ・プロバイダ101は実際の使用、ユーザの識別名、コンテンツ113が実行された回数に基づいてコンテンツ113の人気を測ることができる。実際の使用測定により、このシステムは、テレビ用のニールセン視聴率方式または電話によるアンケート調査など、一度に限られた数のユーザのみをサンプリングし、その結果を推断の基礎とするサンプリング方法を使用するシステムに比べ、より事実主導型のものになる。本実施形態では、電子デジタル・コンテンツ・ストア103またはコンテンツ・プロバイダ101などの指定のウェブ・サイトにログオンするユーザについて、実際の使用を測定することができる。

【0376】4. 暗号化解除1505、圧縮解除1506、再生1506の各コンポーネント

これらのコンポーネントでは、コピー/再生管理コンポーネントが取得したキーを使用してデータ管理およびライブラリ・アクセスの各コンポーネントから取得したオーディオ・データをアンロックし、適切な圧縮解除を適用してそれを再生用に準備し、システム・オーディオ・サービスを使用してそれを再生する。代替実施形態では、データ管理およびライブラリ・アクセスの各コンポーネントから取得したオーディオ・データをCD、ディスク、テープ、またはミニディスクなどの取外し可能媒体にコピーすることができる。

【0377】5. データ管理1502およびライブラリ・アクセス1503の各コンポーネント

これらのコンポーネントは、エンドユーザのシステム上で様々な記憶装置で歌曲データを記憶して取り出すと同時に記憶した歌曲に関する情報を求める要求を処理するために使用する。

【0378】6. アプリケーション間通信コンポーネント1508

このコンポーネントは、セキュア・デジタル・コンテンツ電子配布プレーヤと、プレーヤ・アプリケーション195を呼び出すことができるかまたはその機能を実行するときにプレーヤ・アプリケーション195が使用する必要があるその他のアプリケーション（たとえば、ブラウザ、ヘルパ・アプリケーション、またはプラグイン

など)との調整のために使用する。たとえば、URL制御が活動化されると、それは適切なブラウザを呼び出し、適切なページをロードするようそれに指示する。

【0379】7. その他の各種コンポーネント
上記のカテゴリ(たとえば、インストール)に該当しない個々のコンポーネントはここにグループ化される。

【0380】8. 汎用プレーヤ

この項では、上記のコンポーネントとプレーヤ・アプリケーション195のあるバージョンとの結合について説明する。プレーヤ・アプリケーション195はソフトウェア・オブジェクトに基づくことによってカスタマイズ用に設計されているので、これは多種多様な可能な例の1つにすぎない。

【0381】プレーヤ・オブジェクト・マネージャ1501は、他のすべてのコンポーネントをまとめて保持するソフトウェア・フレームワークである。上記の各項で述べたように、この図でプレーヤ・オブジェクト・マネージャ1501の下にあるブロックはどのプレーヤにも必要であるが、使用する暗号化またはスクランブルの形式、オーディオ圧縮のタイプ、コンテンツ113のライブラリ用のアクセス方法などに応じて専用バージョンと置き換えることができる。

【0382】プレーヤ・オブジェクト・マネージャ1501の上には変数オブジェクト1512があり、これはたいいてい再生またはサーチ中のコンテンツ113に関連するメタデータから導出される。これらの変数オブジェクトは、エンドユーザ表示1510によりエンドユーザ装置109に使用可能なものになり、エンドユーザ・コントロール1511から入力を受け取る。すべてのオブジェクトは構成可能であり、すべてのコンテナのレイアウトはカスタマイズ可能である。これらのオブジェクトは、C/C++、Java、またはそれと同等のプログラミング言語で実現することができる。

【0383】プレーヤ・アプリケーション195の使用以下の実施形態は、エンドユーザ装置109上で実行されるプレーヤ・アプリケーション195がオーディオ・プレーヤであり、コンテンツ113が音楽である例に関するものである。ただし、当業者であれば、他のタイプのコンテンツ113もプレーヤ・アプリケーション195によってサポートできることに留意されたい。典型的なオーディオ・マニアは複数歌曲を保持するCDのライブラリを持っている。これらのすべては、セキュア・デジタル・コンテンツ電子配布システム100内で使用可能なものである。電子デジタル・コンテンツ・ストア103から購入された歌曲セットは自分のシステム上のデジタル・コンテンツ・ライブラリ196内に記憶される。物理的なCDに類似した歌曲のグループ化は再生リストとして記憶される。場合によっては、再生リストが1枚のCDを正確にエミュレートする(たとえば、1枚の市販のCDのすべてのトラックがそのCDのオン

ライン・バージョンとして電子デジタル・コンテンツ・ストア103から購入され、そのCDのものと同等の再生リストによって定義される)。しかし、ほとんどの再生リストは、エンドユーザが自分のシステム上のデジタル・コンテンツ・ライブラリに記憶した歌曲をグループ化するために、エンドユーザによってまとめられる。しかし、以下の説明のため、再生リストという用語に言及するときは、オーダメイドの音楽CDの例を使用する。

10 【0384】SCプロセッサ192アプリケーションからの呼出しにより始動させるのではなく、エンドユーザがプレーヤ・アプリケーション195を明示的に開始すると、それは最後にアクセスした再生リストにプリロードされる。デジタル・コンテンツ・ライブラリ196にいかなる再生リストも存在しない場合、再生リスト・エディタが自動的に開始される(ユーザが優先設定によりこの機能をオフにしていない場合に限る)。詳細については以下の再生リストを参照されたい。

20 【0385】プレーヤ・アプリケーション195は特定の歌曲を引数として指定して呼び出すこともでき、その場合、そのアプリケーションは直ちに歌曲再生モードに入る。任意選択で、その歌曲は、再生用に準備することができるが、処理の前にエンドユーザによるアクションを待つ可能性がある。このような状況の詳細については以下の歌曲再生を参照されたい。

【0386】再生リスト(エンドユーザ・インタフェース1603の対応画面): エンドユーザが再生リスト機能呼び出したときに、以下の機能が使用可能になる。

・ 再生リストのオープン

30 ・ デジタル・コンテンツ・ライブラリを呼び出して、選択のために記憶した再生リストのリストを表示する。詳細については以下のデジタル・コンテンツ・ライブラリも参照されたい。

・ 再生リストの編集

・ すでにロードされている場合は現行再生リストを提供して、再生リスト・エディタ(以下を参照)を呼び出す。そうでない場合は、エディタは始めに空の再生リストを作成する。

・ 再生リストの実行

40 ・ 選択した歌曲(どの歌曲も選択されない場合は再生リストの先頭)から始めて、一度に1曲ずつ歌曲を再生する。再生リスト・エディタに設定されたオプションは再生の順序付けを左右する。しかし、再生リストのこの再生に関するオプションを指定変更するために、ここではいくつかのコントロールが用意されている。

・ 歌曲の再生

・ 再生リストから選択した歌曲のみ再生する。詳細については以下の歌曲再生を参照されたい。

・ 再生リスト情報

50 ・ 再生リストに関する情報を表示する。

- ・ 歌曲情報
- ・ 再生リスト内の選択した歌曲に関する情報を表示する。
- ・ ウェブ・サイトの訪問
- ・ この再生リストに関連するウェブ・サイトをブラウザにロードする。
- ・ ライブラリ
- ・ デジタル・コンテンツ・ライブラリ・ウィンドウをオープンする。詳細については以下のデジタル・コンテンツ・ライブラリも参照されたい。
- 【0387】再生リスト・エディタ（エンドユーザ・インタフェース1603の対応画面）：再生リスト・エディタを呼び出す場合、エンドユーザのオプションは以下の通りである。
- ・ 再生リストの閲覧／ロード／削除
- ・ デジタル・コンテンツ・ライブラリを呼び出して、ロードまたは削除するものを選択するために、記憶した再生リストのリストを表示する。詳細については以下のデジタル・コンテンツ・ライブラリも参照されたい。
- ・ 再生リストの保管
- ・ 再生リストの現行バージョンをデジタル・コンテンツ・ライブラリ196に保管する。
- ・ 歌曲の削除
- ・ 現在選択した歌曲を再生リストから削除する。
- ・ 歌曲の追加
- ・ 再生リストに追加する歌曲を選択するために、歌曲サーチ・モードでデジタル・コンテンツ・ライブラリを呼び出す。詳細については以下のデジタル・コンテンツ・ライブラリも参照されたい。
- ・ 歌曲情報の設定
- ・ 再生リスト内の選択した歌曲に関する情報を表示し、それに対する変更を可能にする。この情報は再生リスト内に記憶され、デジタル・コンテンツ・ライブラリ196内に記憶した歌曲に関する情報は変更しない。以下の項目を変更することができる。
- ・ 表示した歌曲タイトル
- ・ 歌曲に関するエンドユーザの注
- ・ 歌曲再生時の導入遅延
- ・ 歌曲再生後の後続遅延
- ・ 再生時の歌曲内の開始点
- ・ 再生時の歌曲内の終点
- ・ ランダム・モード用の重み付け
- ・ この歌曲用のボリューム調整など
- 【0388】再生リスト属性の設定：この再生リストの属性を表示し、それに対する変更を可能にする。以下の属性を設定することができる。
- ・ 再生リスト・タイトル
- ・ 再生リスト・モード（ランダム、順次など）
- ・ 反復モード（1回再生、完了時に再始動など）

- ・ この再生リストに関するエンドユーザの注
- ライブラリ（エンドユーザ・インタフェース1601の対応画面）
- ・ デジタル・コンテンツ・ライブラリ・ウィンドウをオープンする。詳細については以下のデジタル・コンテンツ・ライブラリも参照されたい。
- 【0389】歌曲再生
- 引数として歌曲を指定してプレーヤ・アプリケーション195を呼び出すかまたは再生リストからまたはデジタル・コンテンツ・ライブラリ内で再生用の歌曲を選択することにより、再生用に歌曲を準備すると、エンドユーザのオプション（エンドユーザ・インタフェース1601の対応画面）は以下の通りである。
- ・ 再生
- ・ 休止
- ・ 停止
- ・ 後退スキップ
- ・ 前進スキップ
- ・ ボリュームの調整
- ・ トラック位置の調整
- ・ 歌詞の閲覧
- ・ クレジットの閲覧
- ・ CDカバーの閲覧
- ・ アーティスト・ピクチャの閲覧
- ・ トラック情報の閲覧
- ・ その他のメタデータの閲覧
- ・ ウェブ・サイトの訪問
- ・ 再生リスト
- ・ ライブラリなど
- 【0390】デジタル・コンテンツ・ライブラリ
- デジタル・コンテンツ・ライブラリは、歌曲または再生リストを選択したときに暗黙のうちに呼び出される場合もあれば（上記を参照）、エンドユーザのシステム上で歌曲ライブラリの管理のためにそれ専用のウィンドウにオープンすることもできる。その場合、エンドユーザのオプションは以下の通りである。
- 歌曲の処理：
- アーティスト、カテゴリ、レーベルなどによる全曲ソート
- アーティスト、カテゴリ、レーベルなどによる歌曲の選択
- 40 現行再生リストへの選択歌曲の追加
- CDへの歌曲のコピー（可能である場合）
- 歌曲の削除
- カテゴリへの歌曲の追加など
- 再生リストの処理：
- 名前別のソート
- カテゴリ別のソート
- キーワードによるサーチ
- 含まれる歌曲タイトルによるサーチ
- 選択した再生リストのロード
- 50 再生リストの名前変更

再生リストの削除

選択した再生リストからのCDの作成（可能である場合）など

【0391】E. 同報通信送達モードのエンドユーザ装置109

1. マルチティア・デジタルTVの実施形態

次に、同報通信送達を使用するエンドユーザ装置109の代替実施形態について説明する。図23に移行すると、同報通信インフラストラクチャによりコンテンツ113を受信するための代替実施形態が示されている。同報通信センタ1802により伝送されるパッケージ2006は、セットトップ・ボックス1804で送受信される。セットトップ・ボックス1804は、以下の図26ないし図31に示すユーザ画面の例示的な図など、GUI（グラフィカル・ユーザ・インタフェース）ジェネレータを使用してGUIを生成する。この実施形態のGUIは、ユーザが閲覧している1次プログラムによる干渉を最小限にするように、透明オーバーレイを生成する。ユーザが選択を行うと、バケット・フィルタ1906によってパッケージが抽出される。セットトップ・ボックス1804は、カタログ情報を収集し、ユーザ・テレビ1806上にビデオ・クリップを表示し、ユーザがパッケージを選択してダウンロードできるようにするアプリケーションを実行する。セットトップ・ボックス1804は、所望のパッケージに関連するセクションを抽出して収集し、そのパッケージを再アセンブルする。エンドユーザ装置109により、ユーザはデジタル・コンテンツを記憶し再生することができる（この場合も「再生」という用語は広い意味で使用する）。セットトップ・ボックス1804は単一の論理モジュールであり、別々のソフトウェア・モジュールで実現することができ、そのモジュールは別々の物理装置上で実行される場合もあれば実行されない場合もある。

【0392】バグ・カタログで伝達される情報に基づいて、セットトップ・ボックス1804は、あらゆる瞬間にユーザが実行可能なアクションを表すアイコンにより部分的にビデオ・クリップにオーバーレイする。ユーザが実行可能な2つの主なアクションは、現在宣伝しているコンテンツをダウンロードするよう要求することと、静的オフラインまたは動的オフライン・カタログをブラウズすることである。セットトップ・ボックス1804は、許されるユーザ・アクションのみの正しいアイコンにより閲覧素材にオーバーレイする。

【0393】ユーザがダウンロードすべきコンテンツを選択した後、セットトップ・ボックス1804は、必要であれば、典型的なユーザ認証／クレジット許可ステップを実行するようサーバに連絡することができる。選択したパッケージが動的オフライン・セットに属する場合、セットトップ・ボックス1804は同報通信センタ1802（ただし、このようなチャンネルが使用可能であ

る場合）に連絡し、選択したパッケージの同報通信を要求する。セットトップ・ボックス1804の要求を受信した後、同報通信センタ1802はその要求を妥当性検査し、所望のパッケージの伝送をスケジューリングする。同報通信センタ1802は、同報通信の肯定応答ならびに選択したパッケージを伝達するカルーセルに関連する同報通信間隔によりセットトップ・ボックス1804に応答する。セットトップ・ボックス1804は、ユーザに対して同報通信間隔を表示し、特定の間隔の選択を要求することができる。

【0394】計画したダウンロード時間になると、セットトップ・ボックス1804は、バグ・カタログに指定されたデジタル・チャンネルにチューニングし、多重化した同報通信ストリームから所望のパッケージ・セクションのフィルタリングを開始する。セットトップ・ボックス1804は、伝送エラーを検出し、破壊されたブロックを抑制する（このメカニズムはたとえば巡回冗長検査にすることができるだろう）。セットトップ・ボックス1804は、マスタ・カタログに含まれるパッケージ記述子情報を使用してそのパッケージを再アセンブルする。動的オフライン・セット内のパッケージのダウンロード成功後、セットトップ・ボックス1804は同報通信センタ1802に通知する。

【0395】また、このシステムは、同報通信センタ1802とセットトップ・ボックス1804との間の個別のユニキャスト・ネットワーク接続を使用して破壊されたセクションの回復を促進する能力も有する。通常、破壊されたセクションの数は少ないので、再伝送されるデータのボリュームは少なく、このため、カルーセル・サイクル全体を待つのは対照的に、ユニキャストまたはマルチキャストを使用してユニキャスト・ネットワーク接続によりこれらのセクションを再伝送の方が高速になる。さらに、このチャンネルによりパッケージ全体をダウンロードする方が高速になるだろうとセットトップ・ボックス1804が判断した場合、そのようにすることもできる。

【0396】バケット・フィルタ1906は、設定周波数またはチャンネルあるいはその他の既知のフィルタリング手段に基づいてバケットをフィルタリングすることができる。カルーセルは、同報通信情報とコンテンツSC640を受け取る。受信機は、同報通信されたバケットをコンテンツSC640、アートワークSC2041、グローバルSC2040用の完全なパッケージ2006に再アセンブルするが、これらのSCはまとめて同報通信SCという。エンドユーザ装置109上で実行されるソフトウェア・アプリケーション1910はセットトップ・ボックス1804からパッケージ2006を受け取った。この実施形態のソフトウェア・アプリケーション1910は、プレーヤ・アプリケーション1911とのインタフェースを取るためにコンテンツ・ホスト・エミュ

レータ1912を開始するデーモンである。コンテンツ・ホスト・エミュレータ1912により、この同報通信インフラストラクチャと、通信インフラストラクチャ（インターネットなど）と、コンピュータ可読媒体で同じプレーヤ・アプリケーション191を使用することができる。プレーヤ・アプリケーション191と、セキュア・コンテナ・プロセッサ191、ヘルパ・アプリケーション193、ウォータマーク193、暗号化解除再暗号化194を含む関連パーツは変更されない。このため、開発者には、この同報通信実施形態と通信実施形態またはコンピュータ可読媒体実施形態用のプレーヤを構築するための1組のAPIおよびツールが提供される。そのうえ、クリアリングハウス・エミュレータ1914により、ユーザが最終会計調停のためにエンドユーザ装置109を元通りクリアリング・ハウス105に接続するまで、トランザクションをログ記録することができる。

【0397】次に図25に移行すると、本発明により図22の代替実施形態によってコンテンツを購入するためにエンドユーザ装置上で実行されるプロセスの流れ図2100が示されている。この流れ図をよりよく理解するために、図26ないし図31を参照することになるが、これは本発明による図22の代替実施形態を使用してテレビ1806上で行うユーザの購入を示す一連の画面ショットである。

【0398】プロセス・フロー2100はステップ2101から始まり、「購入」および「カタログ」アイコンが表示される。ステップ2104でユーザ入力を受け取る。ステップ2106および2108では、プログラム2204の同報通信中に「購入」または「カタログ」のユーザ選択を判定するためのテストを行う。「購入」を選択した場合、ステップ2110で請求のために自分自身を識別するようユーザに要求する。ステップ2110～2116および図28に示す実施形態では、「スマート・カード」と関連の個人識別番号（PIN）を使用する。デビット・カードの使用を含む、その他の請求メカニズムも可能である。ユーザが自分自身を識別すると、ステップ2118でダウンロードが開始する。ステップ2106で「カタログ」を選択した場合、ステップ2120で購入可能な製品のメニュー・パネルを表示し、ユーザは選択カーソルによりその製品間をナビゲートすることができる（ステップは図示せず）。ステップ2122でユーザ入力を受け取る。この入力が「購入」である場合、ビューアは認証プロセス2110～2116を続行する。入力が「終了」である場合、ビューアはステップ2126で「購入」および「カタログ」の選択に戻る。認証が成功すると、図30に示すように、ダウンロード・プロセスは任意選択のメッセージがビューアに対してこれを示すことから始まる。ただし、消費者の購入活動によって中断されないビデオの上にすべてのグラフ

ィック・イメージがオーバーレイされることに留意されたい。

【0399】当業者であれば、本発明の同報通信実施形態により以下のものが可能になることに留意されたい。

- ・ デジタル・テレビ放送インフラストラクチャによるデジタル・コンテンツの高速かつ確実なダウンロード（デジタル・コンテンツが後で再生するためのユニットとしてダウンロードすべきパッケージである場合、どのような形式の撮取および解釈も示すように「再生」は広い意味で使用する）

- ・ デジタル・テレビ放送インフラストラクチャによるデジタル・コンテンツの独立した記述。このシステムにより、コンテンツ受信側からコンテンツ送信側への戻りチャンネルが使用不能である（または、滅多に使用可能にならない）ときに、デジタル・テレビ放送インフラストラクチャによるデジタル・コンテンツのダウンロードが可能になる。

- ・ コンテンツ受信側からコンテンツ送信側への戻りチャンネルが使用可能であるときに、ダウンロード時間の改善

- ・ デジタル・テレビ放送インフラストラクチャに接続されたデジタル・セットトップ・ボックス1804とTVを使用して、ユーザがデジタル・コンテンツを選択しダウンロードすること

- ・ 同時にビデオ・プログラムを見ながら、ユーザがデジタル・コンテンツを選択しダウンロードすること

- ・ グラフィックおよびビデオを使用して、コンテンツ・プロバイダがダウンロード用に使用可能なデジタル・コンテンツをプロモーションすること

- ・ マネージャがダウンロード用に使用可能なデジタル・コンテンツの数およびタイプをリアルタイムで更新すること

【0400】2. 個別チャンネルによるウェブ同報通信の実施形態

次に、本発明の同報通信送達によりウェブ同報通信サービス内の個別チャンネルを使用するエンドユーザ装置109の代替実施形態について説明する。図31に移行すると、ウェブ同報通信インフラストラクチャ内の個別チャンネルを使用してコンテンツ113を受信する代替実施形態が示されている。図32は、本発明により図31の代替実施形態によってコンテンツを購入するためにエンドユーザ装置上で実行されるプロセスの流れ図2800である。セットトップ・ボックス1804は、以下の図33ないし図42に示すユーザ画面の例示的な図など、ウェブ・ストア2306が構築したウェブ・ページを受け取る。

【0401】図33ないし図42の例示的なユーザ画面に関連して図32の流れ図2800を使用する説明を以下に示す。このプロセスは、ステップ2802でウェブ・キャスト・チャンネルによりプロモ・キャッシュ232

10

20

30

40

50

2にプロモーション素材をダウンロードすることから始まる。ユーザが「アルバム・リスト」と表示されたボタンを選択した場合、ステップ2806で図33に示すような選択リストが提示される。この例では、「Madonna」、「Fleetwood Mac」、「Jewel」という3つの選択肢が可能である。これより多くの選択肢またはこれより少ない選択肢を表示することができるが、ここでは一例を示しているだけである。ユーザが「Madonna」などを選択した場合、ステップ2810では、図34に示すようにそのアーティストに関する詳細が提示される。ただし、「サンプル」ボタンによって音楽のサンプルをレビューできることに留意されたい。ユーザが「サンプル」ボタンを選択すると、ウェブ・ブラウザ191によるかあるいはプレーヤ・アプリケーション191により、プロモーション・クリップが再生される。ユーザが選択肢の購入を選択した場合、ステップ2812および2814では、図35に示すように「口座」および「パスワード」を検証するための画面が提示される。この例では、コンテンツ113のプロバイダが決定するように、会計情報をウェブ・ストア2306と同期させるかまたはクリアリング・ハウス105と同期させることができる。キャッシュ・マネージャ2320はアルバム+DSCバッファ2324を検査して、対応するコンテンツSC630がローカルで検索用に使用可能であるかどうかを判定する。正しいコンテンツSCが使用可能である場合、それは取り出され、選択を処理するためにプレーヤ・アプリケーション195に渡される。対応するコンテンツSC630が使用不能である場合、キャッシュ・マネージャ2320は次のコンテンツSC630の同報通信に加入する。音楽の例に戻ると、同報通信およびダウンロードは「Madonna Material Girl」という選択肢である。図36に示すようにキャッシュ・マネージャ2320が正しいダウンロード・チャンネルおよび時間をスケジューリングすると、追加の任意選択情報を含む画面がユーザに提示される。

【0402】ユーザが「自分の選択」を選択した場合、図37とステップ2816および2818に示すように、キャッシュ・マネージャ2320がウェブ同報通信によりダウンロードするようスケジューリングした選択肢のリストが示される。この例では、ユーザはコンテンツ113の第2のピースを購入するプロセスを繰り返す。コンテンツ113の第2のピースは「Fleetwood Mac Greatest Hits」である。次にユーザには、前述のようにステップ2804、2806、2808、2810、2814のプロセス・フローに対応する図38ないし図40が提示される。この時点ですでにユーザによって2つの選択肢が選択されているが、「自分の選択」ボタンが選択されると、ユーザには図41の「Madonna」および「Fleetwood Mac」という2つの項目の状況が提示されるが、各選択ごとに1つずつ、2通りの状況が示

されることに留意されたい。「Fleetwood Mac」に関する状況は「送達予定」である。「Madonna」に関する状況は「送達済み」であり、「ライブラリに追加」ボタンが示される。ユーザが「ライブラリに追加」ボタンと、対応するコンテンツSC631と、ユーザが「切断」であるとき、すなわち、同報通信センタ2302から同報通信を受信しないときにこのプロセスを行えることを強調するためにここで呼び出されたDSCとを選択すると、ステップ2822、2824、2826で、トリガ・マネージャ2326アプリケーションが始動し、アルバム+DSCバッファ2324からその選択肢用のコンテンツSC631を取り出し、それを処理のためにプレーヤ・アプリケーション195に送る。コンテンツSC631を受け取ると、プレーヤ・アプリケーション195は「接続」実施形態に関して前述したようにコンテンツ113を使用する。一実施形態のプレーヤ・アプリケーション195は、インターネットなどのバック・チャンネルを使用して、会計情報についてクリアリング・ハウス105と調停する。図42は、「Madonna」というタイトルがエンドユーザ装置109上のライブラリ196に追加される例である。ライセンスSC147は、インターネットまたはその他の通信ネットワークや同報通信を含むか、または物理的メーラを介し、ディスク、DVD、スマート・カード、デビット・カード、またはCDなどの任意のコンピュータ可読媒体を使用するエンドユーザ装置109に伝送することができる。このプロセス・フロー2800はステップ2830で終了する。

【0403】個別同報通信チャンネル実施形態によるこのウェブ同報通信では、オファーSC641などのプロモーション素材を注文しブラウズするためにユーザを接続する必要がないことに留意されたい。むしろ、プロモーション素材はユーザが「切断」またはオフラインで閲覧するためにエンドユーザ装置109上にローカルに記憶される。

【0404】本発明の特定の実施形態を開示してきたが、当業者であれば、本発明の精神および範囲から逸脱せずにこの特定の実施形態に変更を加えることができることに留意されたい。したがって、本発明の範囲はこの特定の実施形態に限定されず、特許請求の範囲が本発明の範囲内のこのような応用例、修正形態、および実施形態をすべて含むことを意図するものである。

【0405】著作権の部分放棄

本特許出願のすべての素材は、米国およびその他の国の著作権法に基づく著作権保護の対象となる。本出願の最初の有効出願日現在で、この素材は未発表のものとして保護される。しかし、米国特許商標局の特許ファイルまたはレコードに現れるような特許文書または特許開示を誰かがファクシミリで複写することに対して著作権オナーの異議がない限り、この素材をコピーするための許可をここに許諾するが、それ以外のものについてはすべて

の著作権を留保する。

【0406】関連出願の相互参照

本出願は、「Multi-Tier Digital TV Programming for Content Distribution」について1999年12月9日に出願され、本出願人に譲渡された非暫定的特許出願第 / 号の一部継続出願である。前述の特許出願は参照によりその全体が本明細書に組み込まれる。

【0407】まとめとして、本発明の構成に関して以下の事項を開示する。

【0408】(1) 複数のチャンネルを備えたウェブ同報通信インフラストラクチャによりユーザのシステムに確実にデータを提供する方法であって、第1の暗号化キーを使用してデータを暗号化するステップと、第2の暗号化キーを使用して第1の暗号化解除キーを暗号化するステップと、少なくともユーザのシステム上で受信するために第1のウェブ同報通信チャンネル上で暗号化データの少なくとも一部に関連するプロモーション・メタデータを同報通信するステップと、第2の同報通信チャンネルにより暗号化データの少なくとも一部を同報通信するステップと、暗号化した第1の暗号化解除キーをコンピュータ可読媒体によりユーザのシステムに転送するステップであって、その暗号化した第1の暗号化解除キーが第2の暗号化キーによって暗号化されているステップとを含む方法。

(2) プロモーション・メタデータを同報通信するステップが、所定の時間間隔で定期的にプロモーション・メタデータを同報通信することを含む、上記(1)に記載の方法。

(3) プロモーション・メタデータを同報通信するステップが、少なくともプロモーション・メタデータをウェブ・ブラウザにより読取り可能なフォーマットに変換するサブステップを含む、上記(1)に記載の方法。

(4) 暗号化データの少なくとも一部を同報通信するステップが、暗号化データの少なくとも一部に関する同報通信時間およびウェブ同報通信チャンネルのスケジュールを同報通信することを含む、上記(1)に記載の方法。

(5) 第2のウェブ同報通信チャンネルにより暗号化データの少なくとも一部を同報通信するステップが、DirecPCMと互換性のあるフォーマットで暗号化データを同報通信することを含む、上記(1)に記載の方法。

(6) プロモーション・メタデータがそのデータに関する同報通信時間のスケジュールを含む、上記(1)に記載の方法。

(7) 複数のチャンネルによりウェブ同報通信インフラストラクチャからユーザのシステム上で確実にデータを受信する方法であって、第1のウェブ同報通信チャンネルからプロモーション・メタデータを受信するステップであって、そのプロモーション・メタデータが受信用使用可能なデータに関するメタ・データであるステップと、

プロモーション・メタデータの少なくとも一部をユーザによる検討用のプロモーション・オフリングにアセンブルするステップと、プロモーション・メタデータに関連して受信すべきデータをユーザによって選択するステップと、第2のウェブ同報通信チャンネルからデータを受信するステップであって、そのデータがプロモーション・メタデータから選択されたデータであり、そのデータが第1の暗号化キーを使用してあらかじめ暗号化されているステップと、コンピュータ可読媒体により第1の暗号化解除キーを受信するステップであって、その第1の暗号化解除キーが第2のウェブ同報通信チャンネルにより受信したデータの少なくとも一部を暗号化解除するキーであるステップとを含む方法。

(8) プロモーション・データの少なくとも一部をアセンブルするステップが、プロモーション・データの少なくとも一部をウェブ・ブラウザにより読取り可能なフォーマットにアセンブルすることを含む、選択するステップが、ウェブ・ブラウザにより選択することを含む、上記(7)に記載の方法。

(9) 選択するステップが、ユーザのシステム上であらかじめ受信され記憶されたプロモーション素材を選択することを含む、上記(7)に記載の方法。

(10) 選択するステップが、選択したデータの次のウェブ同報通信に関するスケジュールを決定するサブステップと、ユーザのシステムを起動して第2のチャンネル上で次のウェブ同報通信を受信するトリガを設定するサブステップとをさらに含む、上記(9)に記載の方法。

(11) 第2のウェブ同報通信チャンネルからデータを受信するステップが、トリガによって提供されたウェブ同報通信チャンネルおよび時間においてプロモーション・メタデータから選択したデータを受信することを含む、上記(10)に記載の方法。

(12) 第2のウェブ同報通信チャンネルからデータを受信するステップが、DirecPCMと互換性のあるフォーマットでデータを受信することを含む、上記(7)に記載の方法。

(13) 第2のウェブ同報通信チャンネルからデータを受信するステップが、ユーザのシステムが選択したデータを受信することを許可されていることをバック・チャンネルにより認可するサブステップを含む、第1の暗号化解除キーを受信するステップが、ユーザのシステムが選択したデータを受信することを許可されている場合にのみ第1の暗号化解除キーを受信することを含む、上記(7)に記載の方法。

(14) 第2のウェブ同報通信チャンネルからデータを受信するステップが、プロモーション・メタデータから選択したデータがユーザのシステム上で受信された場合に、次にユーザがユーザのシステムを起動するときにユーザに状況を通知するサブステップをさらに含む、上記(7)に記載の方法。

(15) 第1の暗号化解除キーを受信するステップが、第2の暗号化キーにより暗号化された第1の暗号化解除キーを受信することを含む、上記(7)に記載の方法。

(16) 第1の暗号化解除キーを受信するステップが、同報通信ストリームにより第1の暗号化解除キーを受信することを含む、上記(15)に記載の方法。

(17) 第2の暗号化解除キーがクリアリングハウスからユーザのシステムに送信される、上記(15)に記載の方法。

(18) 第2の暗号化解除キーが、クリアリングハウスからユーザのシステムに送信された第2の暗号化キーにより暗号化されたデータを暗号化解除するタイムアウト設備を有する、上記(15)に記載の方法。

(19) 複数のチャンネルを備えたウェブ同報通信インフラストラクチャによりユーザのシステムに確実にデータを提供するシステムであって、コンテンツ・システムと、第1の公開キーと、第1の公開キーに対応する第1の秘密キーと、データ暗号化キーと、データ暗号化キーを使用して暗号化したデータを暗号化解除するデータ暗号化解除キーと、データ暗号化解除キーのみによって暗号化解除可能になるようにデータを暗号化する第1のデータ暗号化手段と、データ暗号化解除キーを暗号化するために第1の公開キーを使用する第2のデータ暗号化手段と、クリアリング・ハウスと、第2のウェブ同報通信チャンネル上で同報通信されるデータに関連するプロモーション・データを第1のウェブ同報通信チャンネル上の1つまたは複数のユーザのシステムに同報通信し、データ暗号化キーにより暗号化したデータを第2の同報通信チャンネル上で同報通信する同報通信センタと、暗号化されたデータ暗号化解除キーをクリアリング・ハウスに転送する第1の転送手段であって、クリアリング・ハウスが第1の秘密キーを所有する第1の転送手段と、第1の秘密キーを使用してデータ暗号化解除キーを暗号化解除する第1の暗号化解除手段と、第2の公開キーと、第2の公開キーに対応する第2の秘密キーと、第2の公開キーを使用してデータ暗号化解除キーを再暗号化する再暗号化手段と、再暗号化されたデータ暗号化解除キーをユーザのシステムに転送する第2の転送手段であって、ユーザのシステムが第2の秘密キーを所有する第2の転送手段と、第2の秘密キーを使用して再暗号化したデータ暗号化解除キーを暗号化解除する第2の暗号化解除手段とを含むシステム。

(20) プロモーション・メタデータがそのデータに関する同報通信時間のスケジュールを含む、上記(19)に記載のシステム。

(21) 複数のチャンネルによりウェブ同報通信インフラストラクチャから確実にデータを受信する、ユーザのシステムであって、第1のウェブ同報通信チャンネルからプロモーション・メタデータを受信する受信機であって、そのプロモーション・メタデータが受信信用に使用可能な

データに関するメタデータである受信機と、プロモーション・メタデータの少なくとも一部をユーザによる検討用に提示する出力装置へのインタフェースと、プロモーション・メタデータに関連して受信すべきデータに関するユーザによる選択を受信する入力装置へのインタフェースと、第2のウェブ同報通信チャンネルからデータを受信するよう受信機を制御する制御装置であって、そのデータがプロモーション・メタデータから選択されたデータであり、そのデータが第1の暗号化キーを使用してあらかじめ暗号化されている制御装置と、コンピュータ可読媒体により第1の暗号化解除キーを受信するインタフェースであって、その第1の暗号化解除キーが第2のウェブ同報通信チャンネルにより受信したデータの少なくとも一部を暗号化解除するキーであるインタフェースとを含むユーザのシステム。

(22) 出力装置がウェブ・ブラウザであり、入力装置がユーザによる選択を受信するためにウェブ・ブラウザに結合されている、上記(21)に記載のユーザのシステム。

(23) 制御装置が、プロモーション・メタデータから導出したスケジュールであって、第2のウェブ同報通信チャンネルからデータを受信するよう受信機を制御するために使用するスケジュールをさらに含む、上記(21)に記載のユーザのシステム。

(24) 受信機が、DirecPCMと互換性のあるフォーマットで同報通信されたデータを受信するよう適合されている、上記(21)に記載のユーザのシステム。

【図面の簡単な説明】

【図1】本発明によるセキュア・デジタル・コンテンツ電子配布システムの概要を示すブロック図である。

【図2】本発明によるセキュア・デジタル・コンテンツ電子配布システムの概要を示すブロック図である。

【図3】本発明によるセキュア・デジタル・コンテンツ電子配布システムの概要を示すブロック図である。

【図4】本発明によるセキュア・デジタル・コンテンツ電子配布システムの概要を示すブロック図である。

【図5】本発明によるセキュア・コンテナ(SC)の一例と関連の図形表現を示すブロック図である。

【図6】本発明によるセキュア・コンテナ(SC)用の暗号化プロセスの概要を示すブロック図である。

【図7】本発明によるセキュア・コンテナ(SC)用の暗号化解除プロセスの概要を示すブロック図である。

【図8】本発明により図1ないし図4のセキュア・デジタル・コンテンツ電子配布システムの権利管理アーキテクチャ用の諸層の概要を示すブロック図である。

【図9】図8のライセンス制御層に適用されたときのコンテンツ配布ライセンス制御の概要を示すブロック図である。

【図10】本発明により図1ないし図4のワーク・フロー・マネージャ・ツール用のユーザ・インタフェースの

10

20

30

40

50

一例を示す図である。

【図 11】本発明により図 10 のユーザ・インタフェースに対応するワーク・フロー・マネージャの主要ツール、コンポーネント、プロセスを示すブロック図である。

【図 12】本発明により図 1 ないし図 4 の電子デジタル・コンテンツ・ストアの主要ツール、コンポーネント、プロセスを示すブロック図である。

【図 13】本発明により図 1 ないし図 4 のエンドユーザ装置の主要コンポーネントおよびプロセスを示すブロック図である。

【図 14】本発明により図 11 のコンテンツ前処理圧縮ツール用のコード化速度係数を計算するための方法の流れ図である。

【図 15】本発明により図 11 の自動メタデータ収集ツール用の追加情報を自動的に検索するための方法の流れ図である。

【図 16】本発明により図 11 の前処理圧縮ツールの前処理圧縮パラメータを自動的に設定するための方法の流れ図である。

【図 17】本発明により図 18 ないし図 19 に記載するようにローカル・ライブラリにコンテンツをダウンロードするプレーヤ・アプリケーションのユーザ・インタフェース画面の一例を示す図である。

【図 18】本発明により図 12 のエンドユーザ装置上で実行されるプレーヤ・アプリケーションの主要コンポーネントおよびプロセスを示すブロック図である。

【図 19】本発明により図 12 のエンドユーザ装置上で実行されるプレーヤ・アプリケーションの主要コンポーネントおよびプロセスを示すブロック図である。

【図 20】本発明により図 18 ないし図 19 のプレーヤ・アプリケーションのユーザ・インタフェース画面の一例を示す図である。

【図 21】本発明により図 11 の自動メタデータ収集ツール用の追加情報を自動的に検索するための代替実施形態の流れ図である。

【図 22】本発明により同報通信インフラストラクチャを使用するデジタル・コンテンツの電子配布の代替実施形態を示す高レベル論理図である。

【図 23】図 22 の詳細ブロック図であり、本発明により同報通信インフラストラクチャを使用するデジタル・コンテンツの電子配布の代替実施形態を示す図である。

【図 24】本発明により図 22 の代替実施形態で同報通信されるバケットのブロック図である。

【図 25】本発明により図 22 の代替実施形態によってコンテンツを購入するためにエンドユーザ装置上で実行されるプロセスの流れ図である。

【図 26】本発明により図 22 の代替実施形態を使用してテレビ上で行われるユーザの購入を示す画面ショット

である。

【図 27】本発明により図 22 の代替実施形態を使用してテレビ上で行われるユーザの購入を示す画面ショットである。

【図 28】本発明により図 22 の代替実施形態を使用してテレビ上で行われるユーザの購入を示す画面ショットである。

【図 29】本発明により図 22 の代替実施形態を使用してテレビ上で行われるユーザの購入を示す画面ショットである。

【図 30】本発明により図 22 の代替実施形態を使用してテレビ上で行われるユーザの購入を示す画面ショットである。

【図 31】図 22 の詳細ブロック図であり、本発明によりウェブ同報通信サービス内の個別チャンネルを使用するデジタル・コンテンツの電子配布の代替実施形態を示す図である。

【図 32】本発明により図 31 の代替実施形態によってコンテンツを購入するためにエンドユーザ装置上で実行されるプロセスの流れ図である。

【図 33】本発明により図 31 の代替実施形態を使用してテレビ上で行われるユーザの購入を示す画面ショットである。

【図 34】本発明により図 31 の代替実施形態を使用してテレビ上で行われるユーザの購入を示す画面ショットである。

【図 35】本発明により図 31 の代替実施形態を使用してテレビ上で行われるユーザの購入を示す画面ショットである。

【図 36】本発明により図 31 の代替実施形態を使用してテレビ上で行われるユーザの購入を示す画面ショットである。

【図 37】本発明により図 31 の代替実施形態を使用してテレビ上で行われるユーザの購入を示す画面ショットである。

【図 38】本発明により図 31 の代替実施形態を使用してテレビ上で行われるユーザの購入を示す画面ショットである。

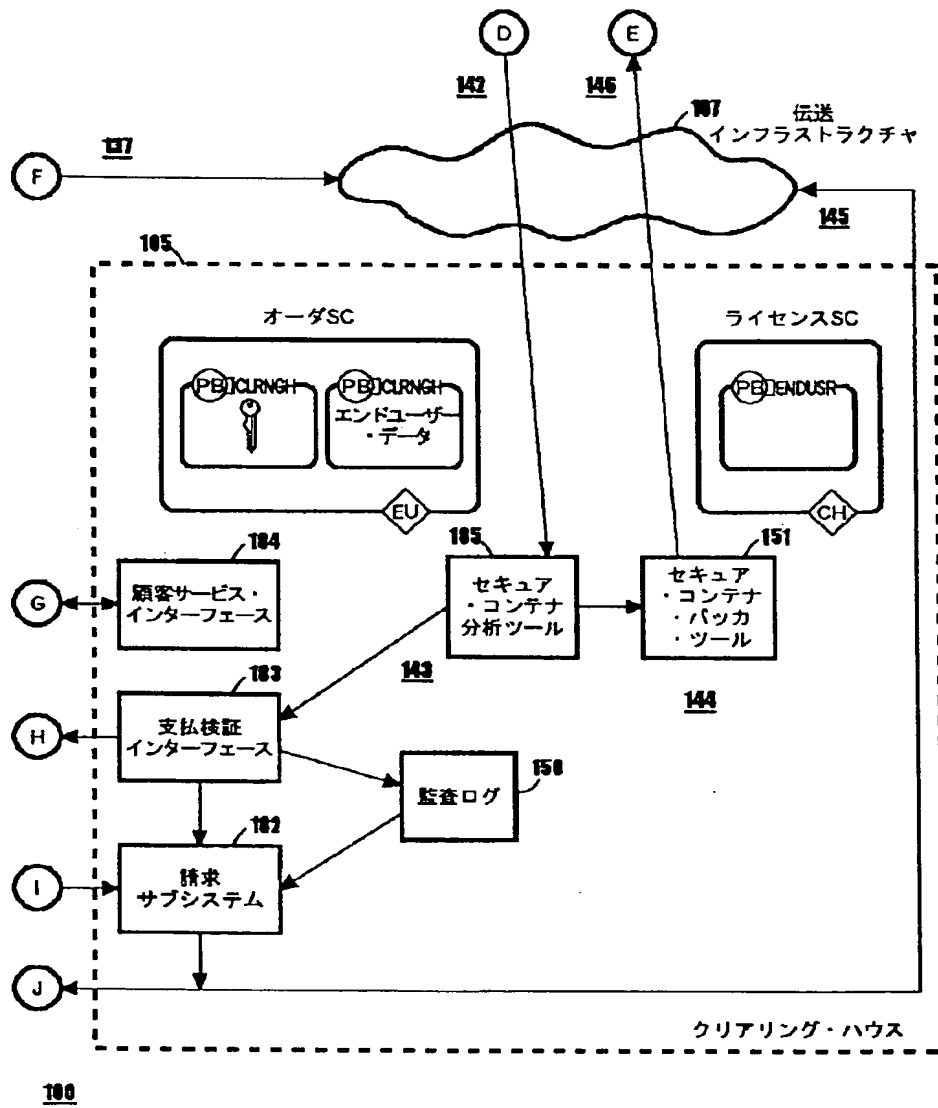
【図 39】本発明により図 31 の代替実施形態を使用してテレビ上で行われるユーザの購入を示す画面ショットである。

【図 40】本発明により図 31 の代替実施形態を使用してテレビ上で行われるユーザの購入を示す画面ショットである。

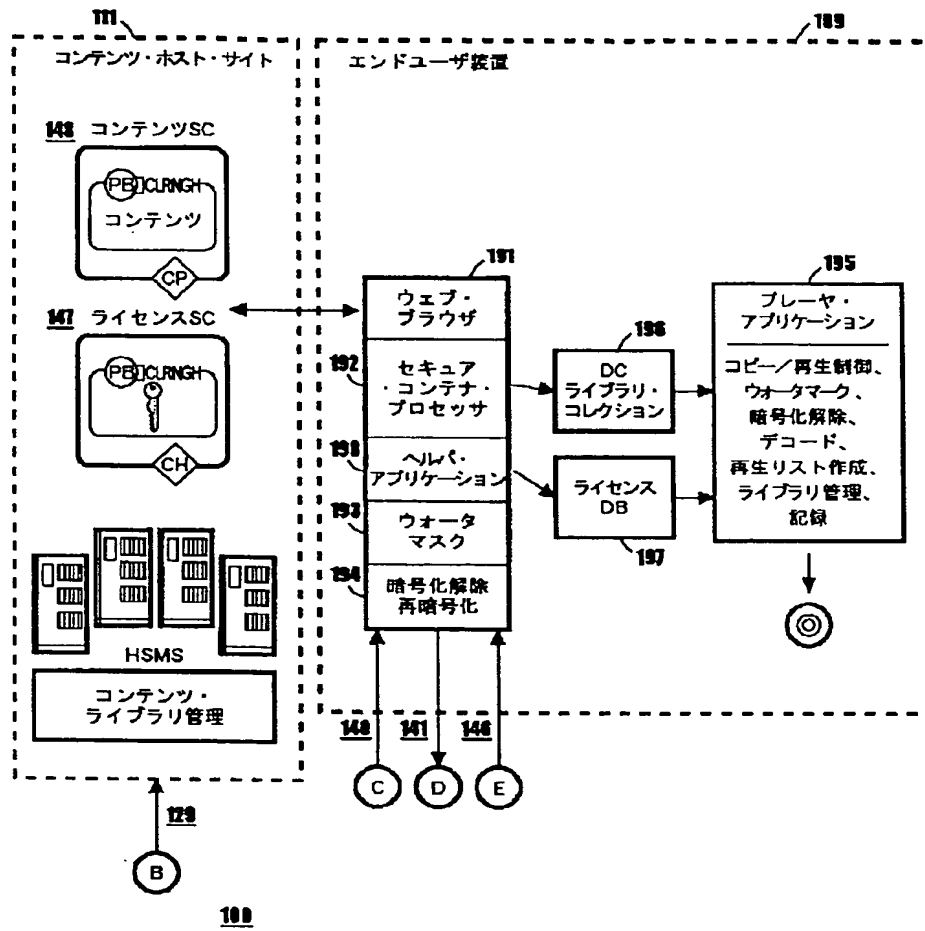
【図 41】本発明により図 31 の代替実施形態を使用してテレビ上で行われるユーザの購入を示す画面ショットである。

【図 42】本発明により図 31 の代替実施形態を使用してテレビ上で行われるユーザの購入を示す画面ショット

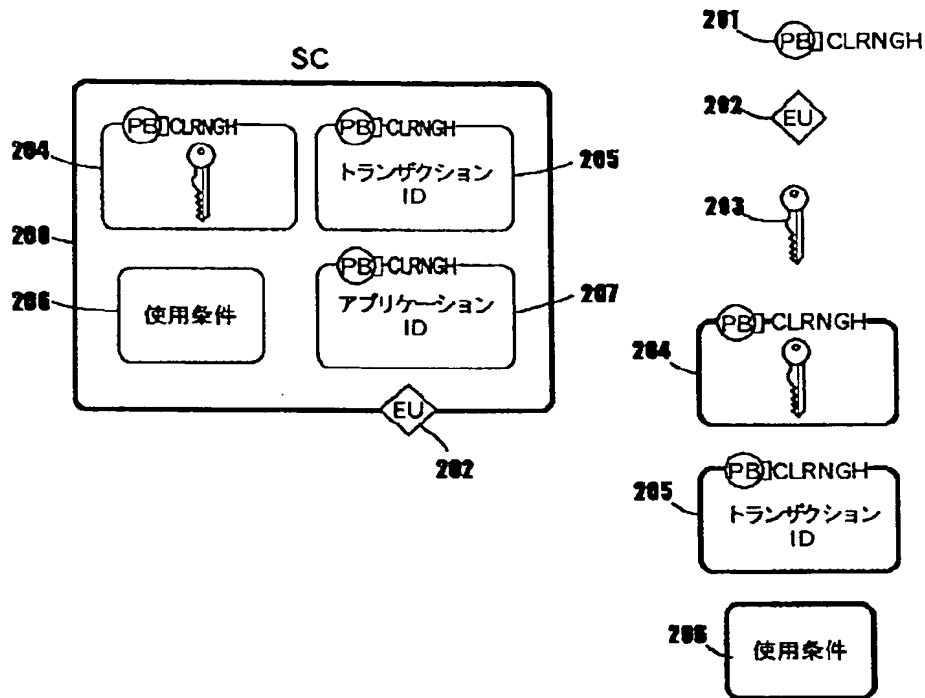
【図3】



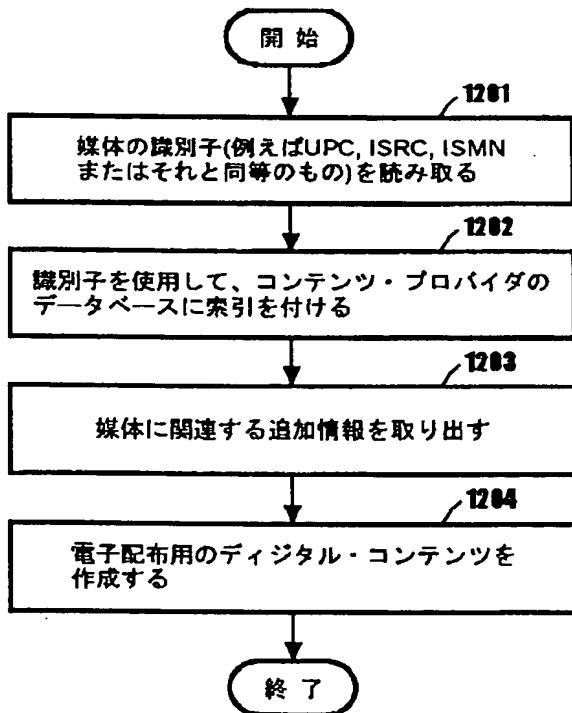
【図4】



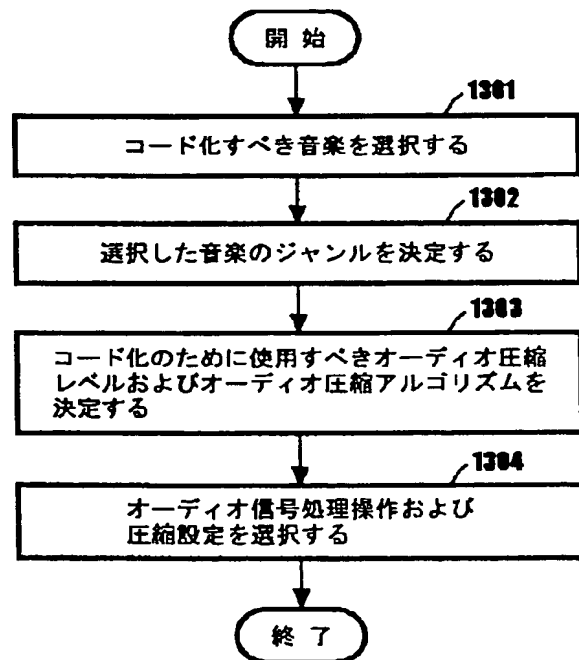
【図5】



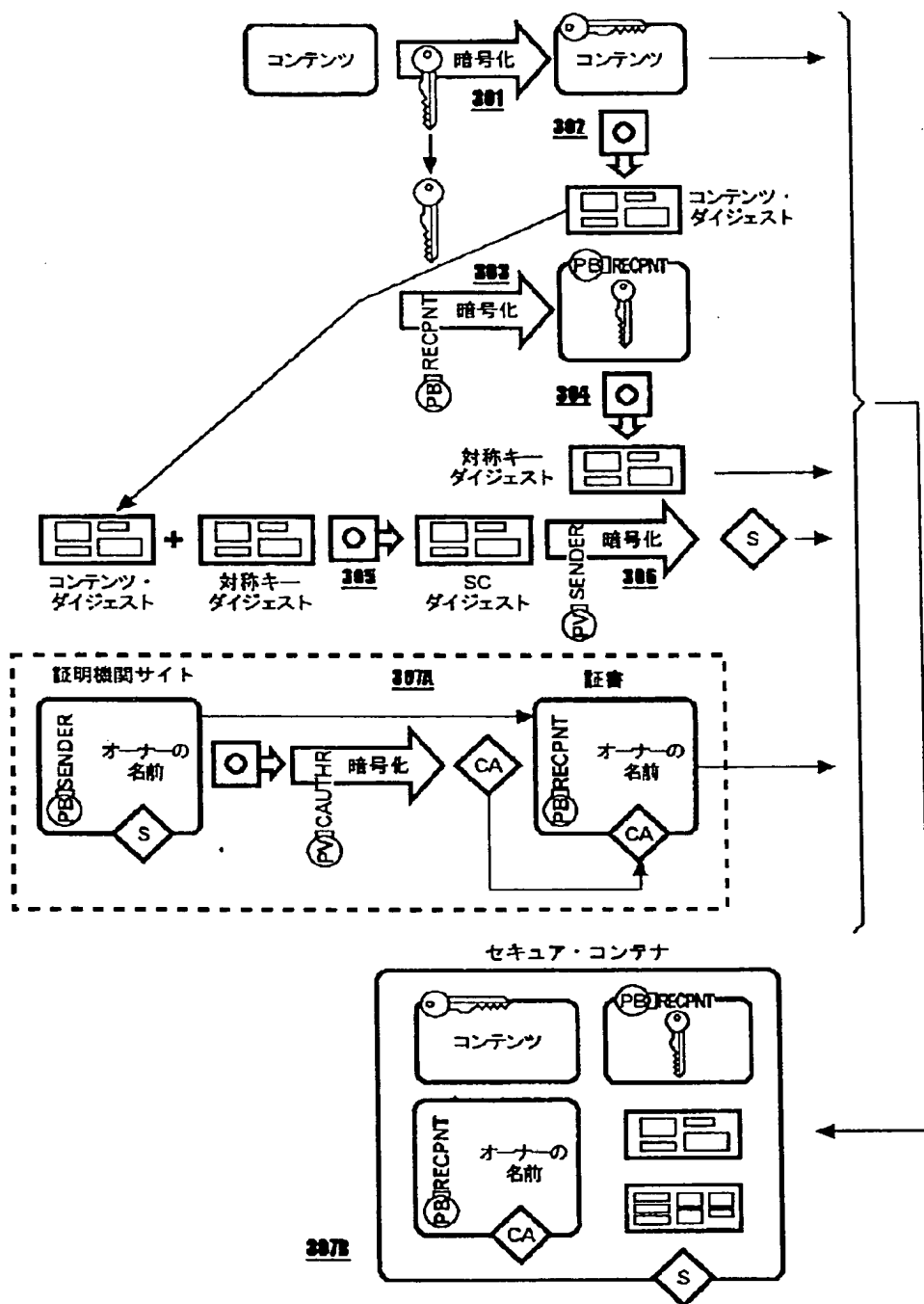
【図15】



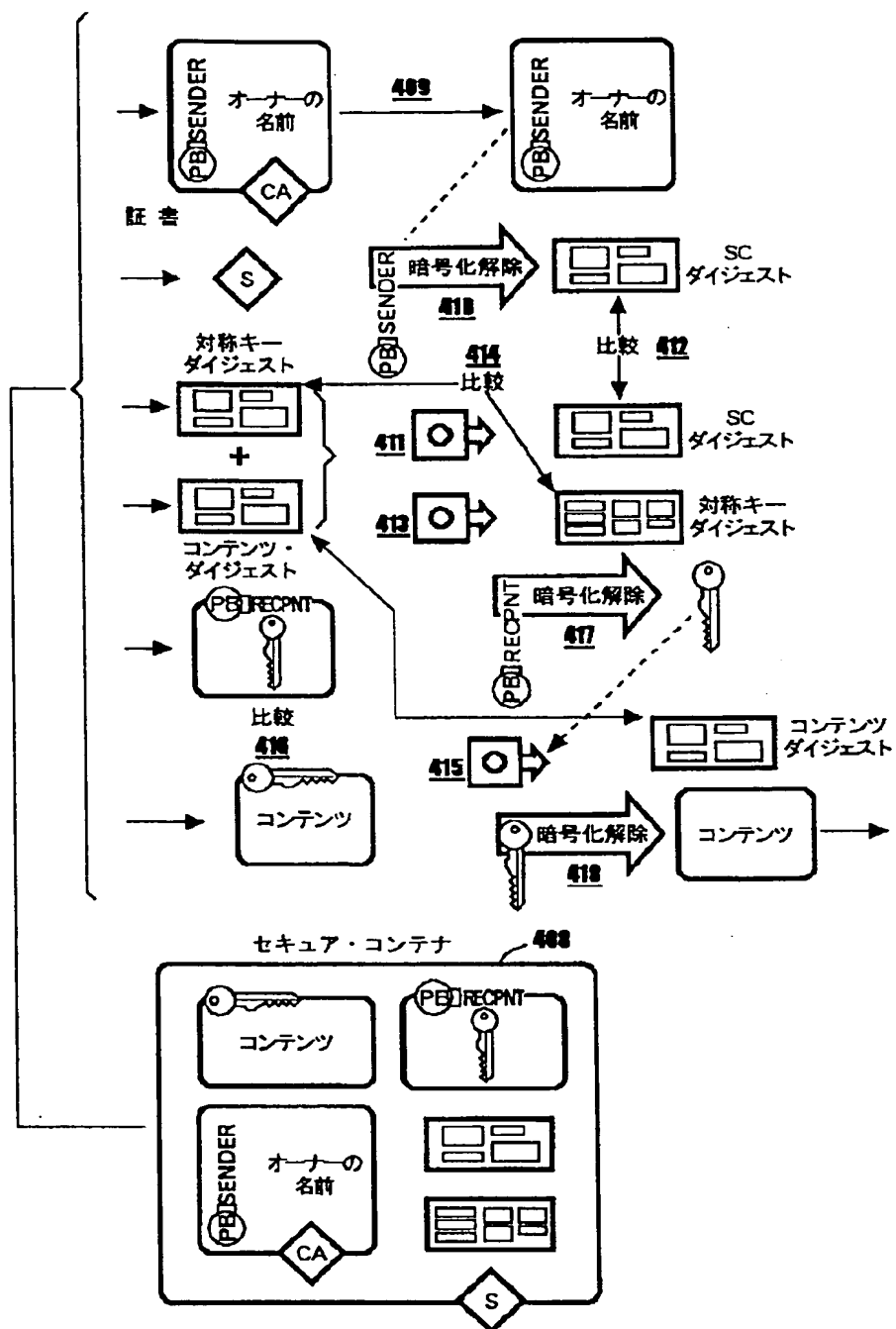
【図16】



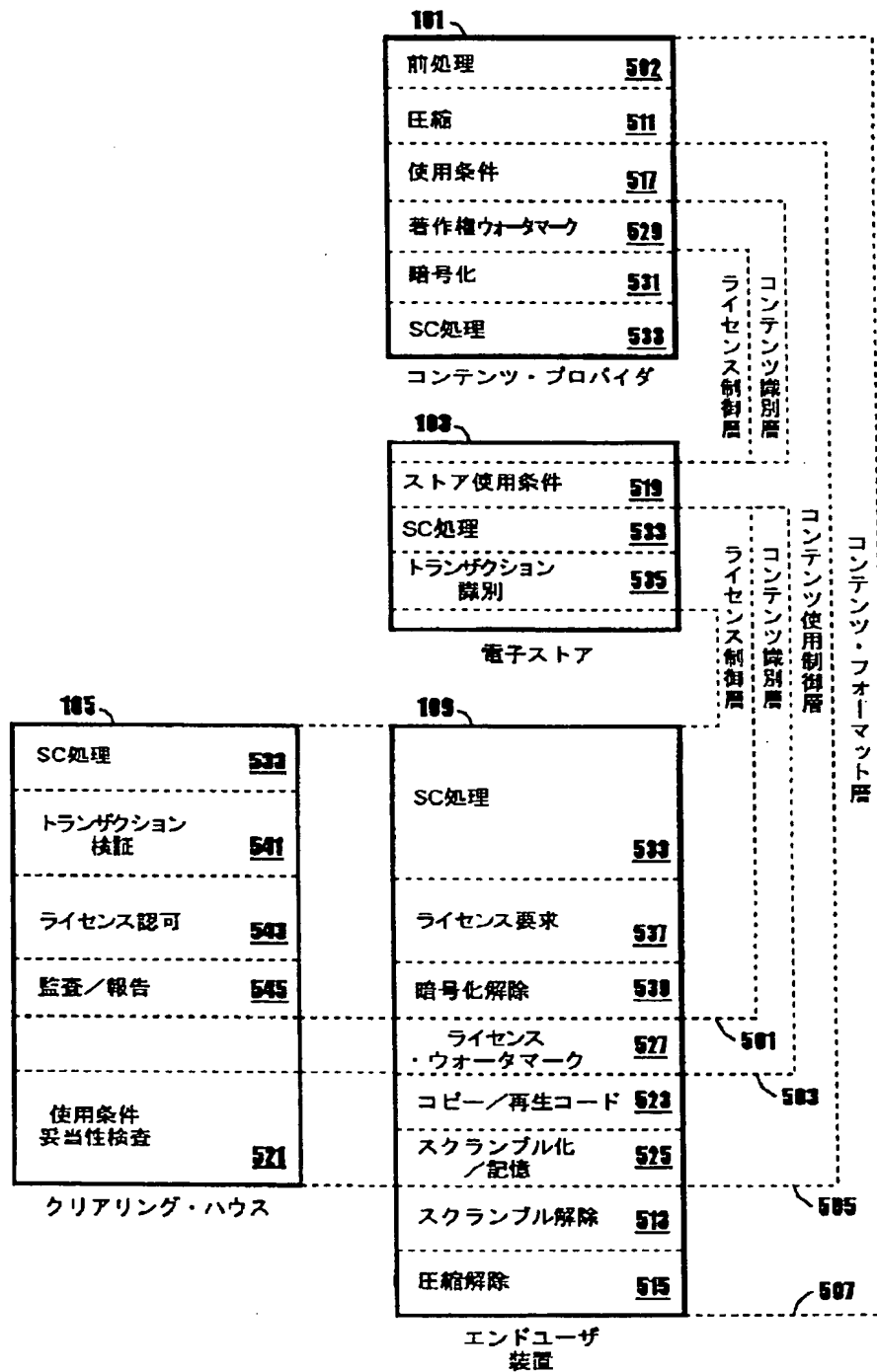
【図6】



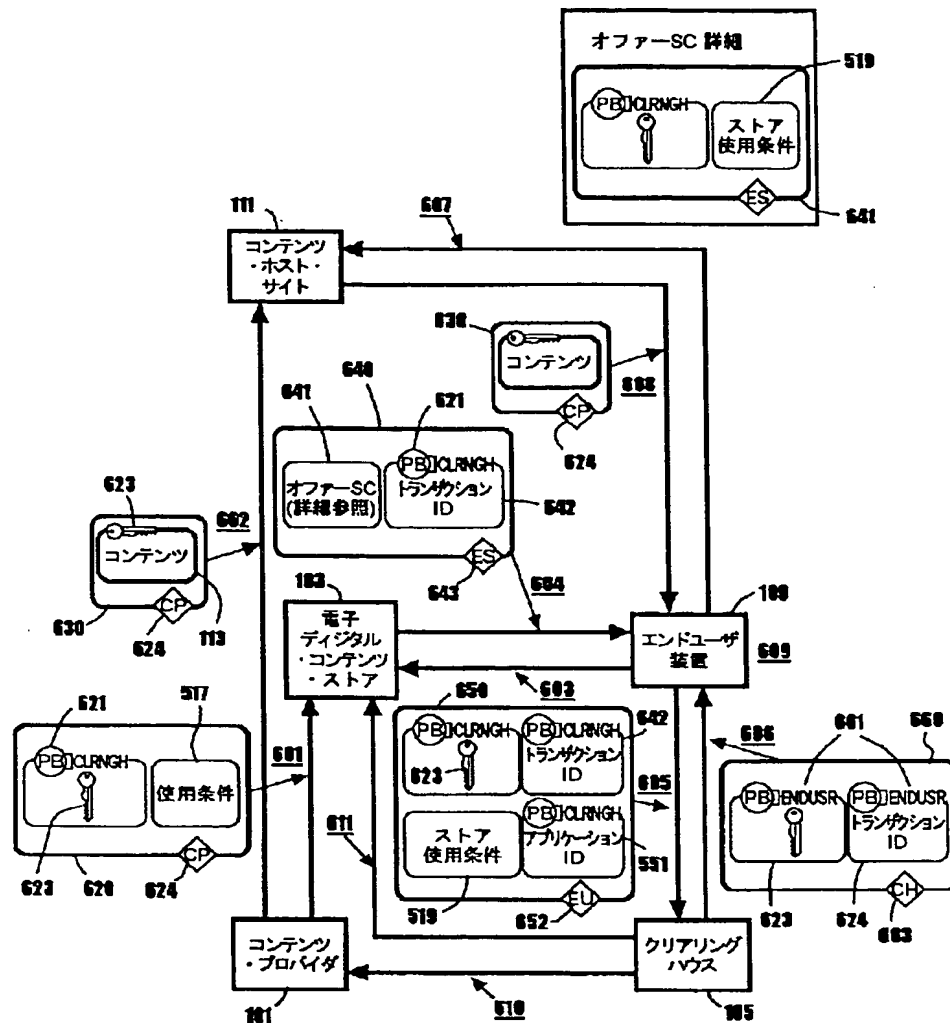
【図7】



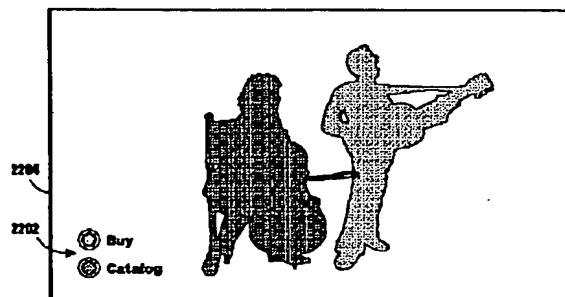
【図8】



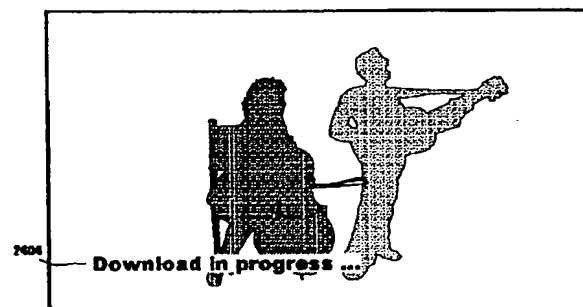
【図9】



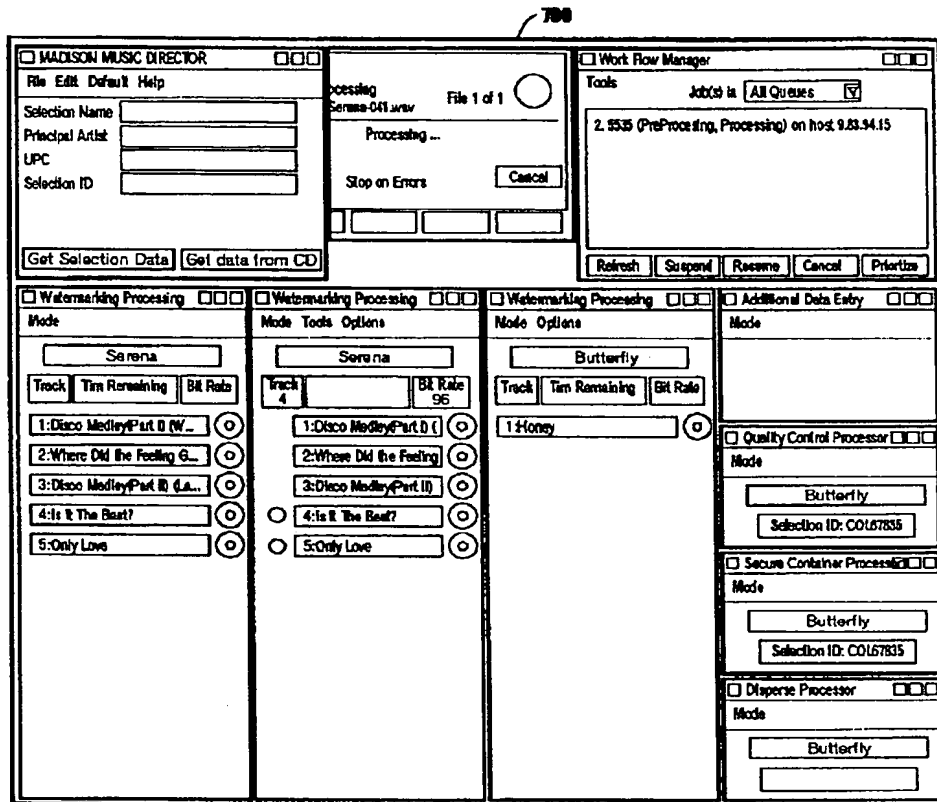
【図26】



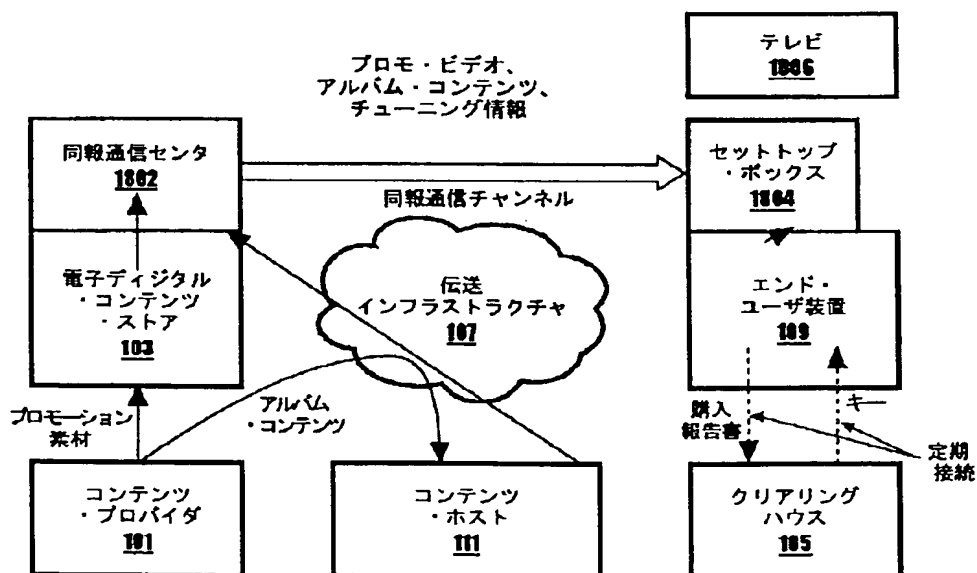
【図28】



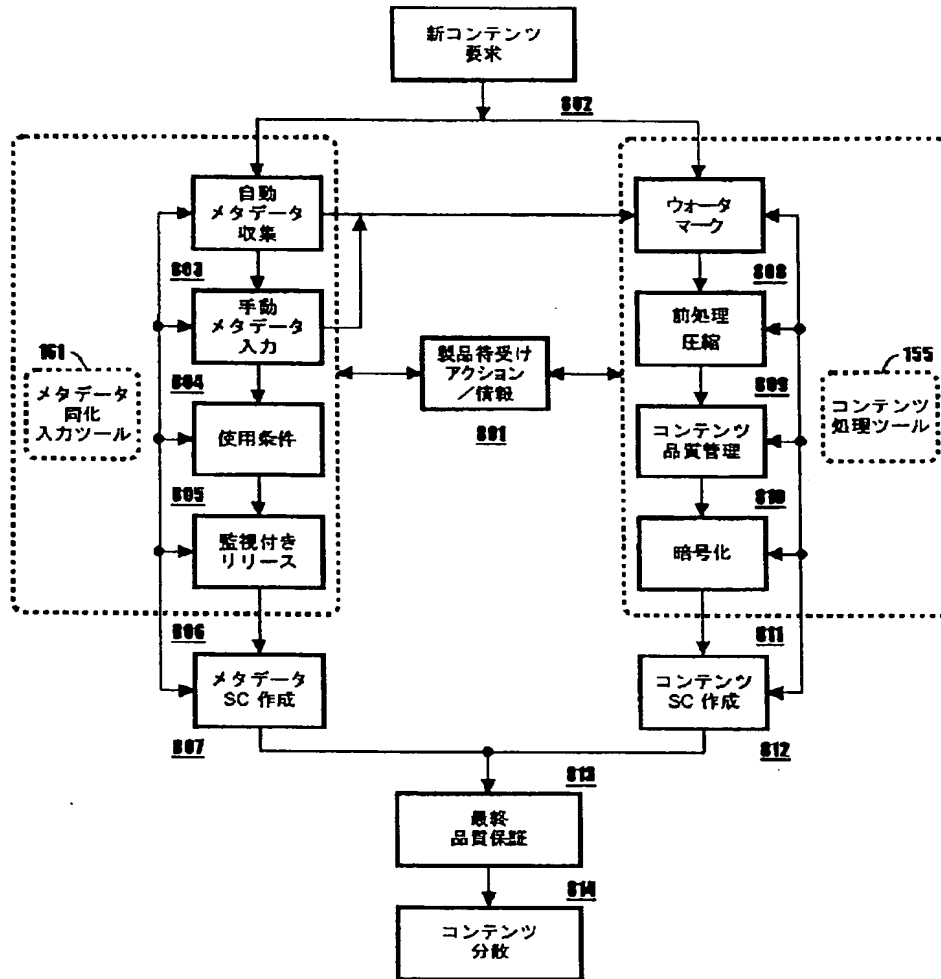
【図10】



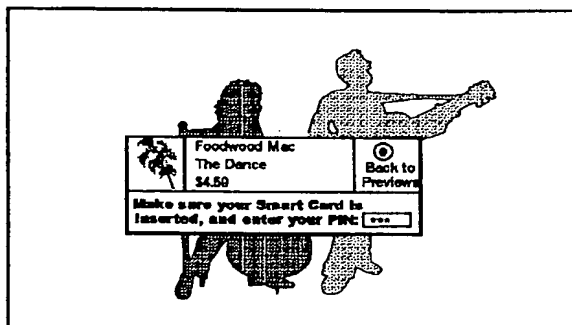
【図22】



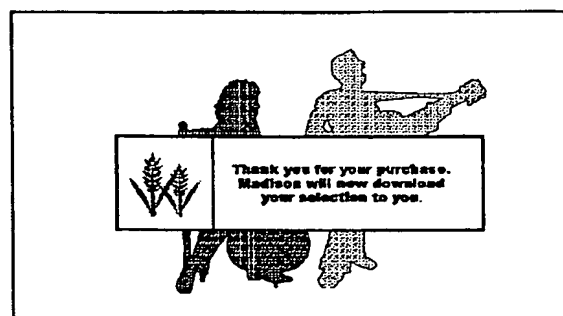
【図11】



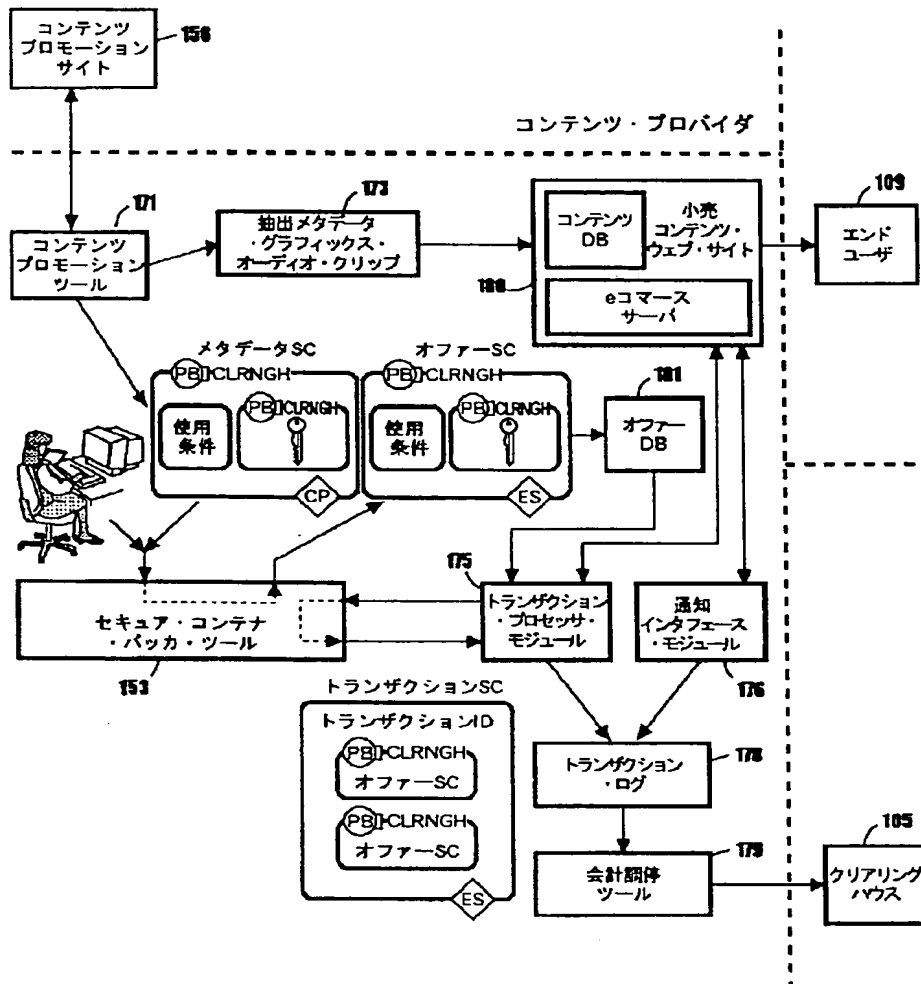
【図29】



【図30】



【図12】



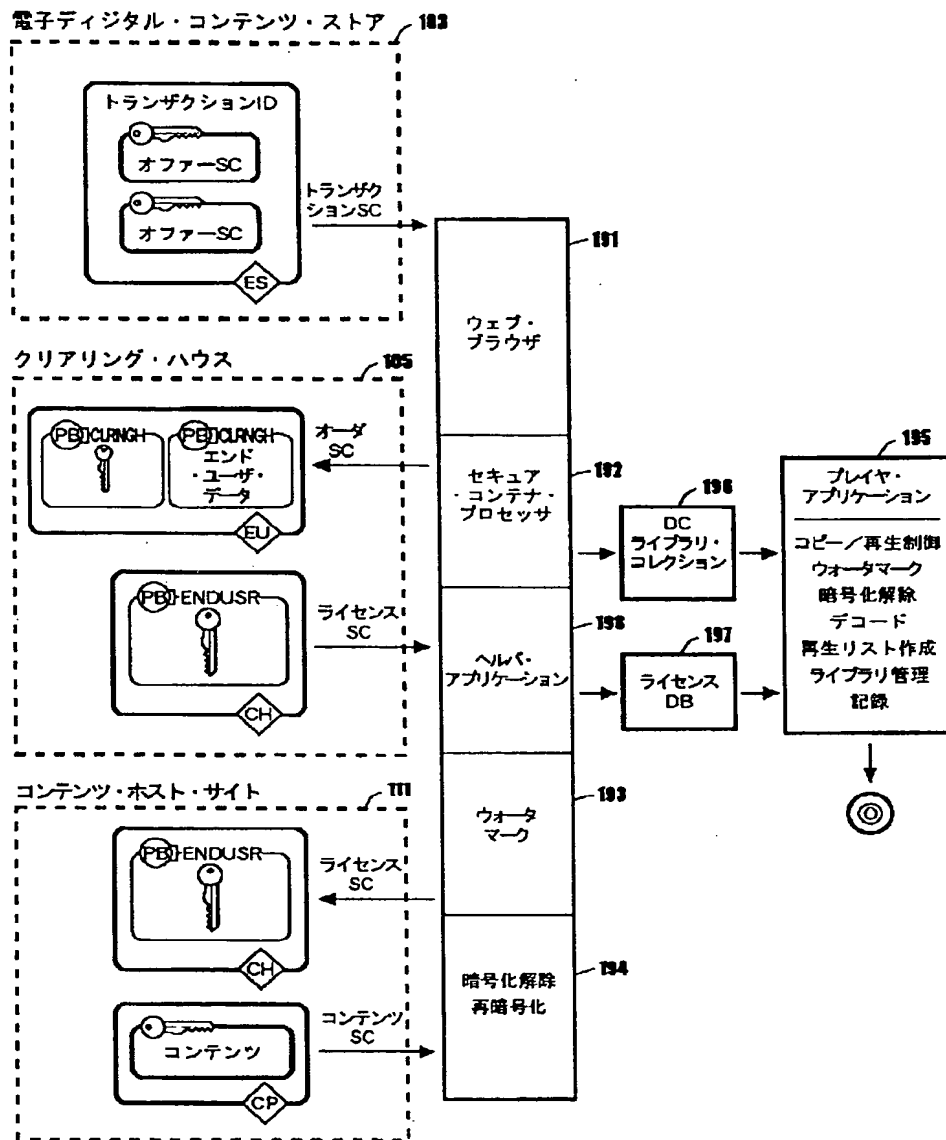
【図33】

Turbo Music	
<div>DirectPC</div> <div> <input type="button" value="My Selections"/> <input type="button" value="Album List"/> <input type="button" value="?"/> </div>	
<div>Home Desc</div> <div>Turbo Internet</div> <div>Turbo Winboard</div> <div>Turbo Winboard</div> <div>Service Station</div> <div>Turbo Music</div>	<div> <div>Sample Cover</div> <div>Marila</div> <div>The Immaculate Collection</div> <div>Select</div> </div> <div> <div>Sample Cover</div> <div>Foodwood Mac</div> <div>Greatest Hits</div> <div>Select</div> </div> <div> <div>Sample Cover</div> <div>Jest</div> <div>Price for You</div> <div>Select</div> </div>

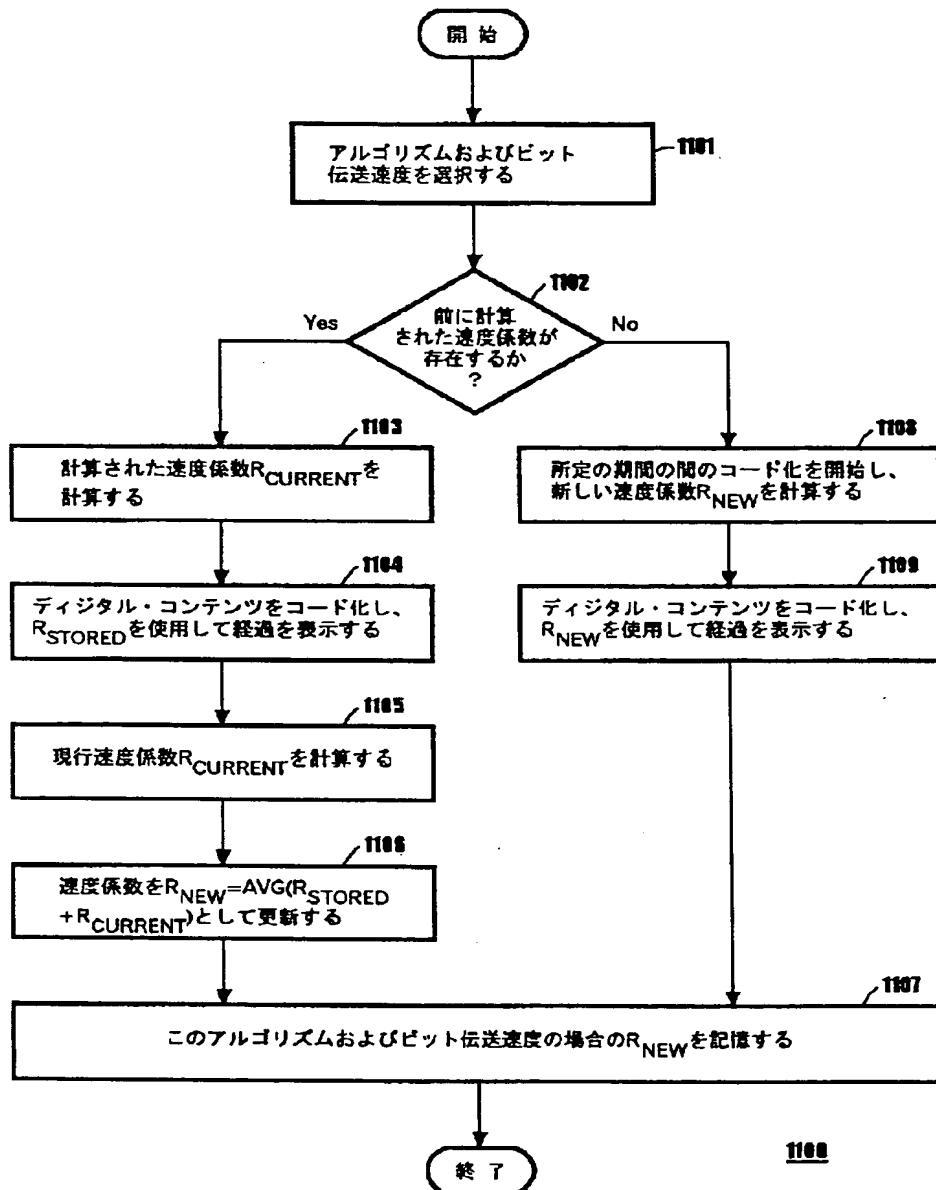
【図34】

Turbo Music	
<div>DirectPC</div> <div> <input type="button" value="My Selections"/> <input type="button" value="Album List"/> <input type="button" value="?"/> </div>	
<div>Home Desc</div> <div>Turbo Internet</div> <div>Turbo Winboard</div> <div>Turbo Winboard</div> <div>Service Station</div> <div>Turbo Music</div>	<div> <div>Sample Cover</div> <div>Marila</div> <div>The Immaculate Collection</div> <div>\$6.95</div> </div> <div> <div>1. Material boy (30sec)</div> <div>Sample</div> </div> <div> <div>2. Hungry (30sec)</div> <div>Sample</div> </div> <div> <div>Order</div> <div>Cancel</div> </div>
<div>DirectPC will deliver this album to you within 2 hours.</div>	

【図13】

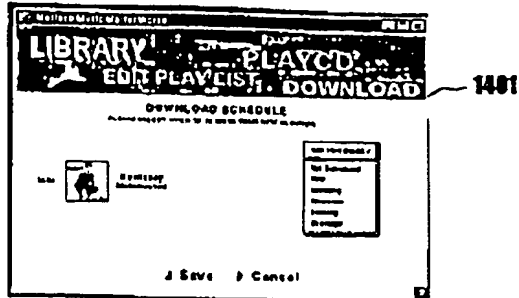


【図14】



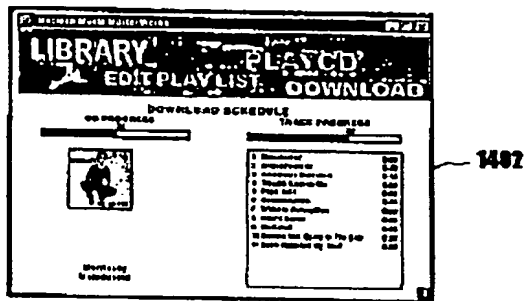
【図17】

ダウンロードのスケジュール



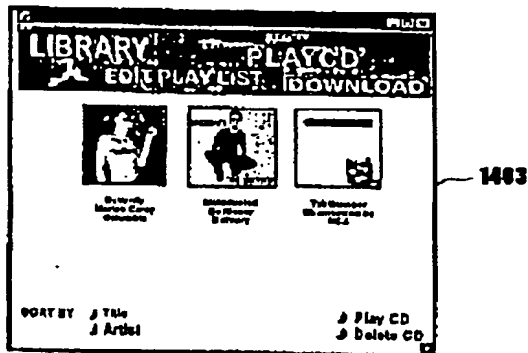
ユーザがダウンロードを
開始する

ダウンロード

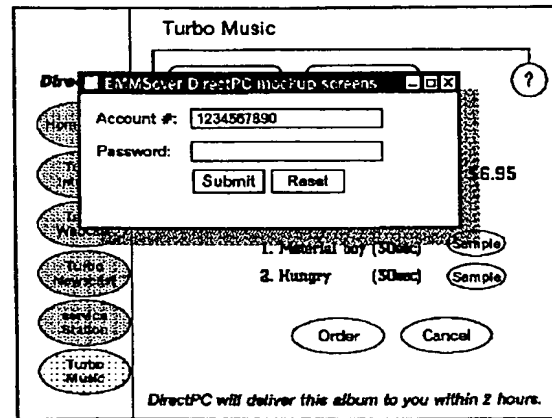


ダウンロードが
完了する

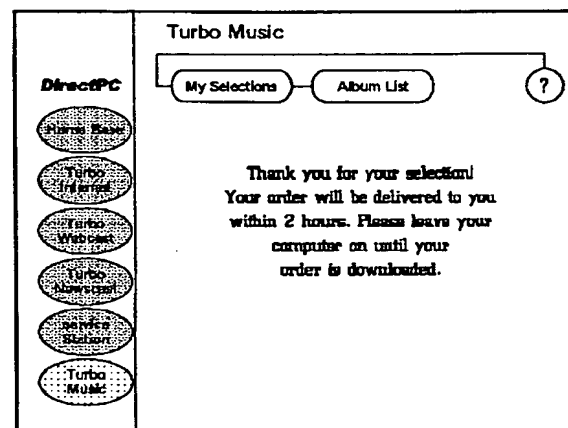
ライブラリ



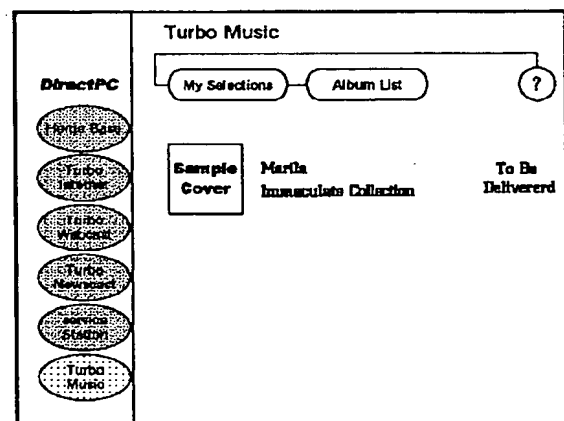
【図35】



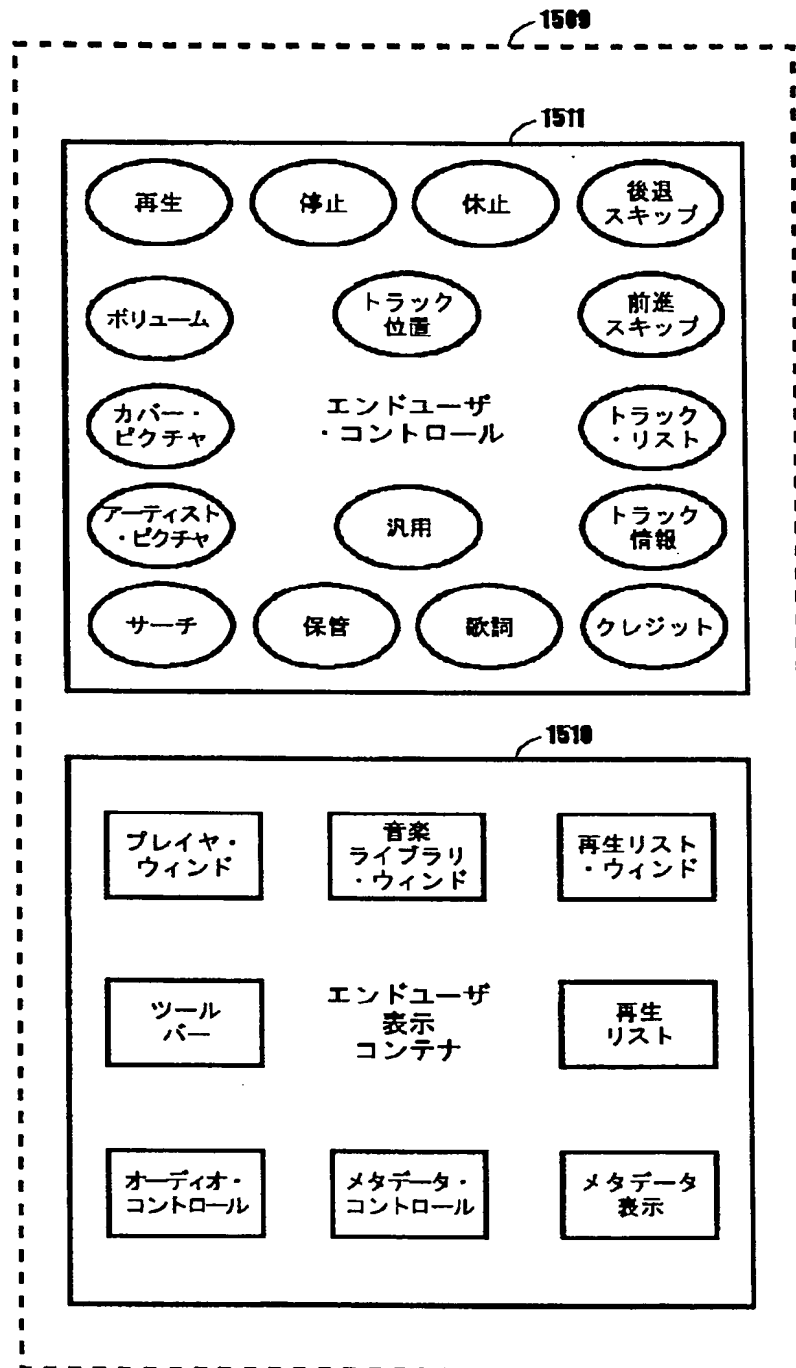
【図36】



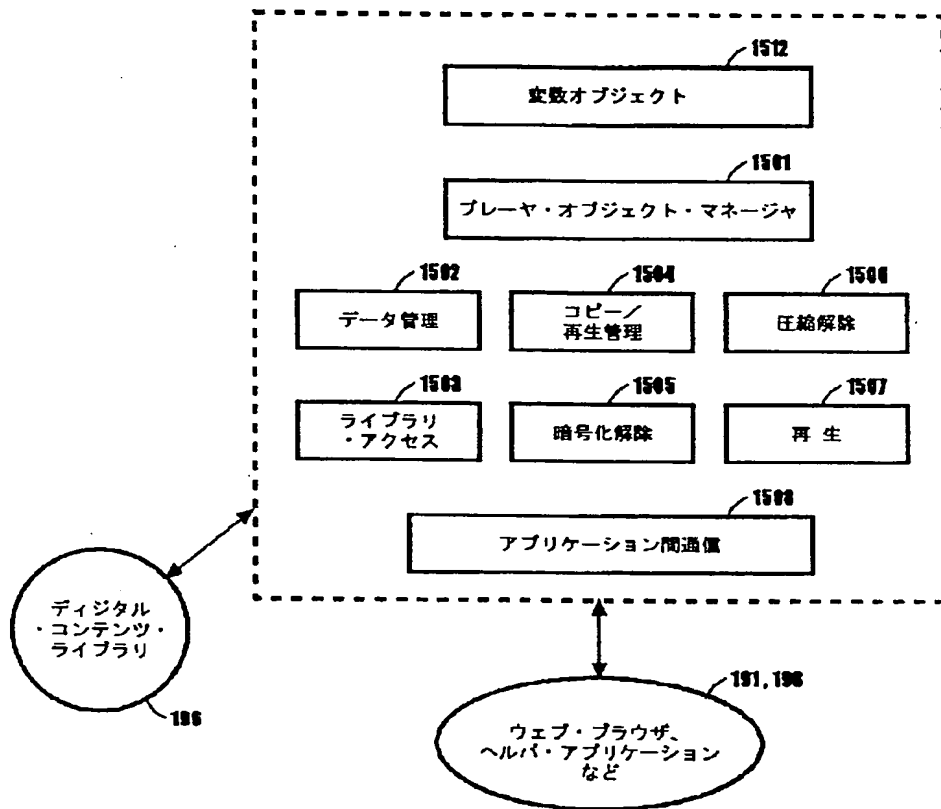
【図37】



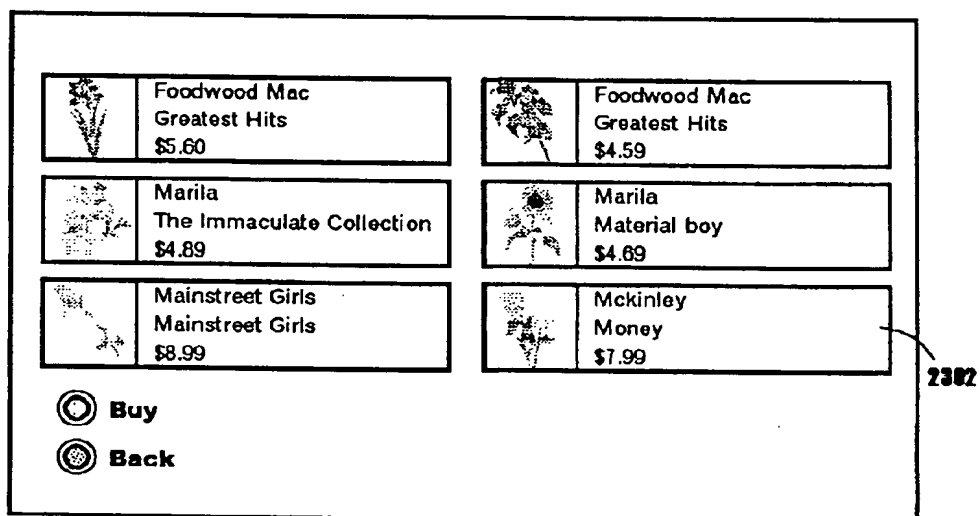
【図18】



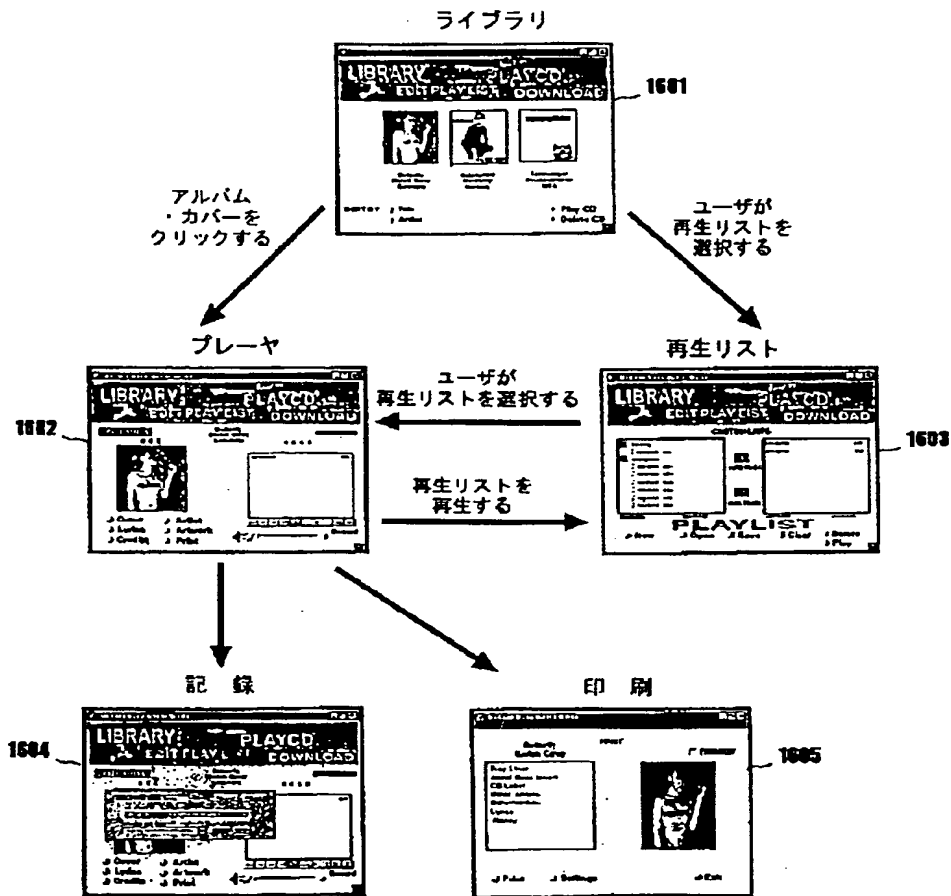
【図19】



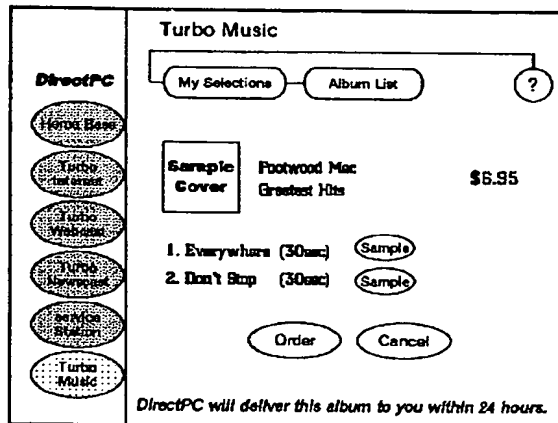
【図27】



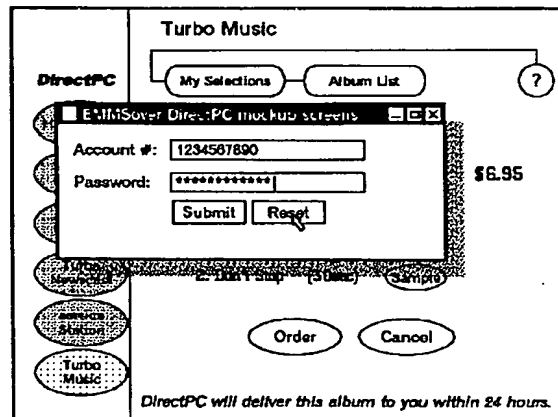
【図20】



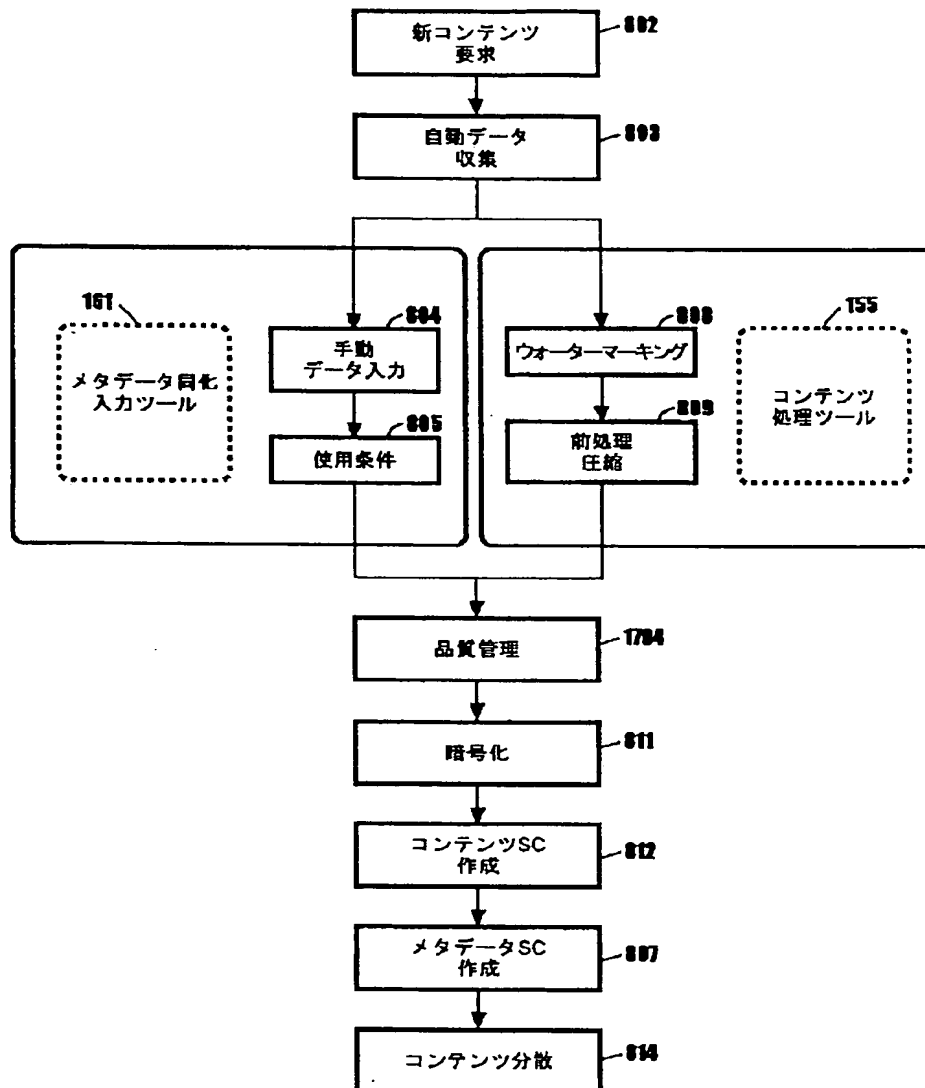
【図38】



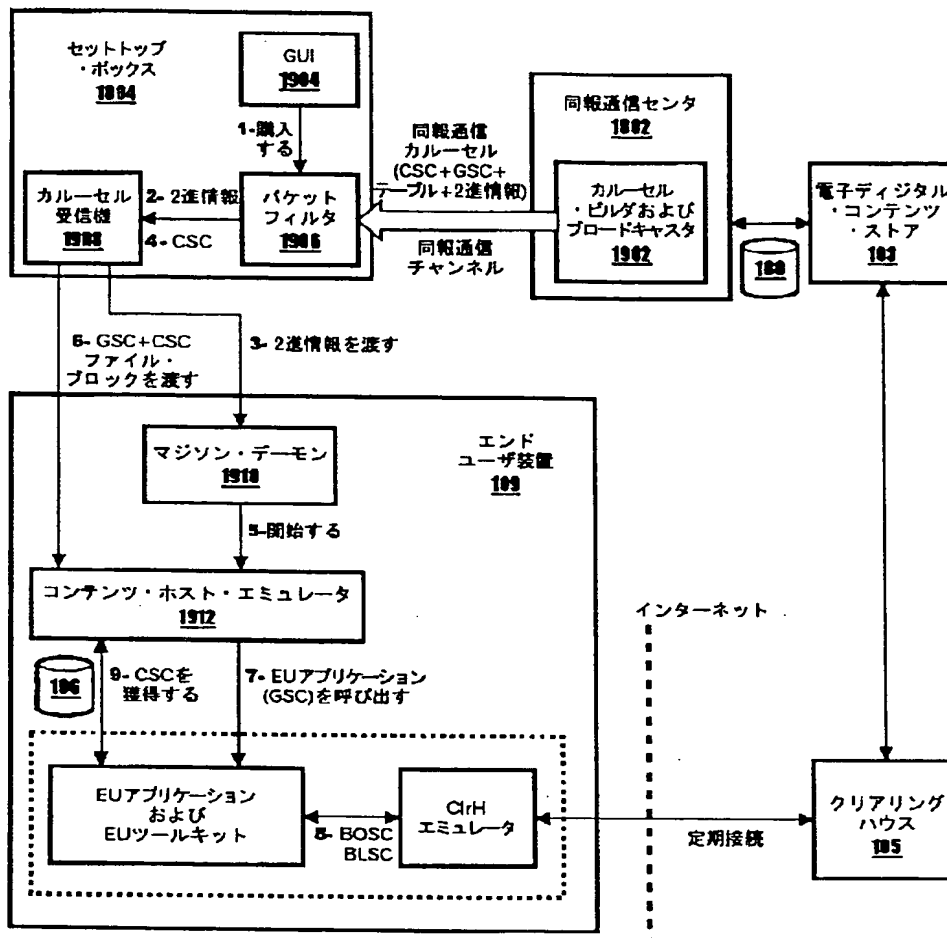
【図39】



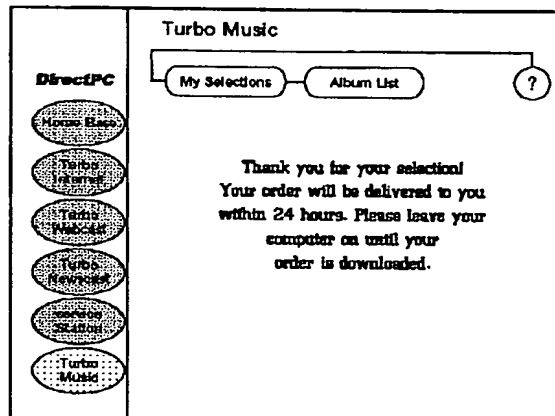
【図21】



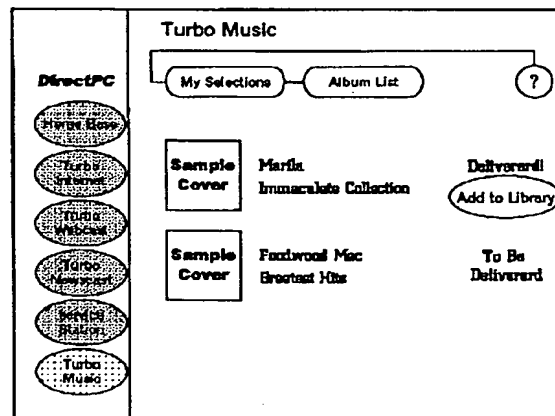
【図23】



【図40】

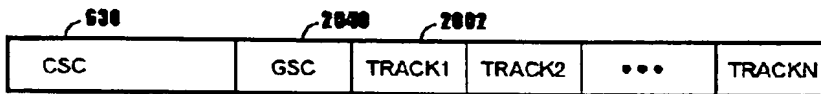


【図41】



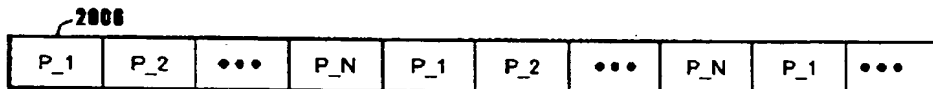
【図24】

パッケージ・フォーマット



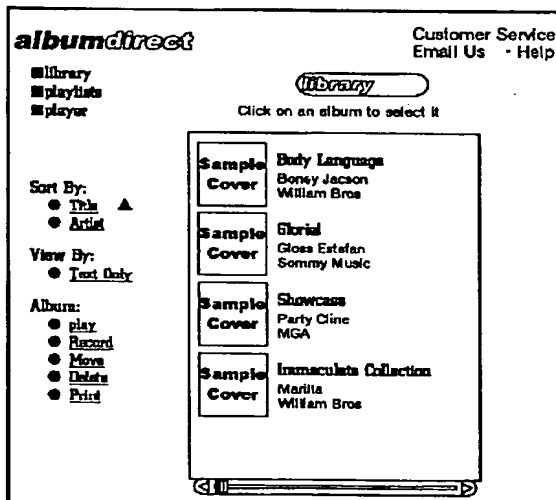
CSC = コンテンツ・セキュア・コンテナ
 GSC = グローバル・セキュア・コンテナ、
 すなわち、各ユーザに毎週配布されるグローバル・キーを使用して
 暗号化されたキーを備えたセキュア・コンテナ
 ASCはアート・ワーク・セキュア・コンテナである

カルーセル・フォーマット

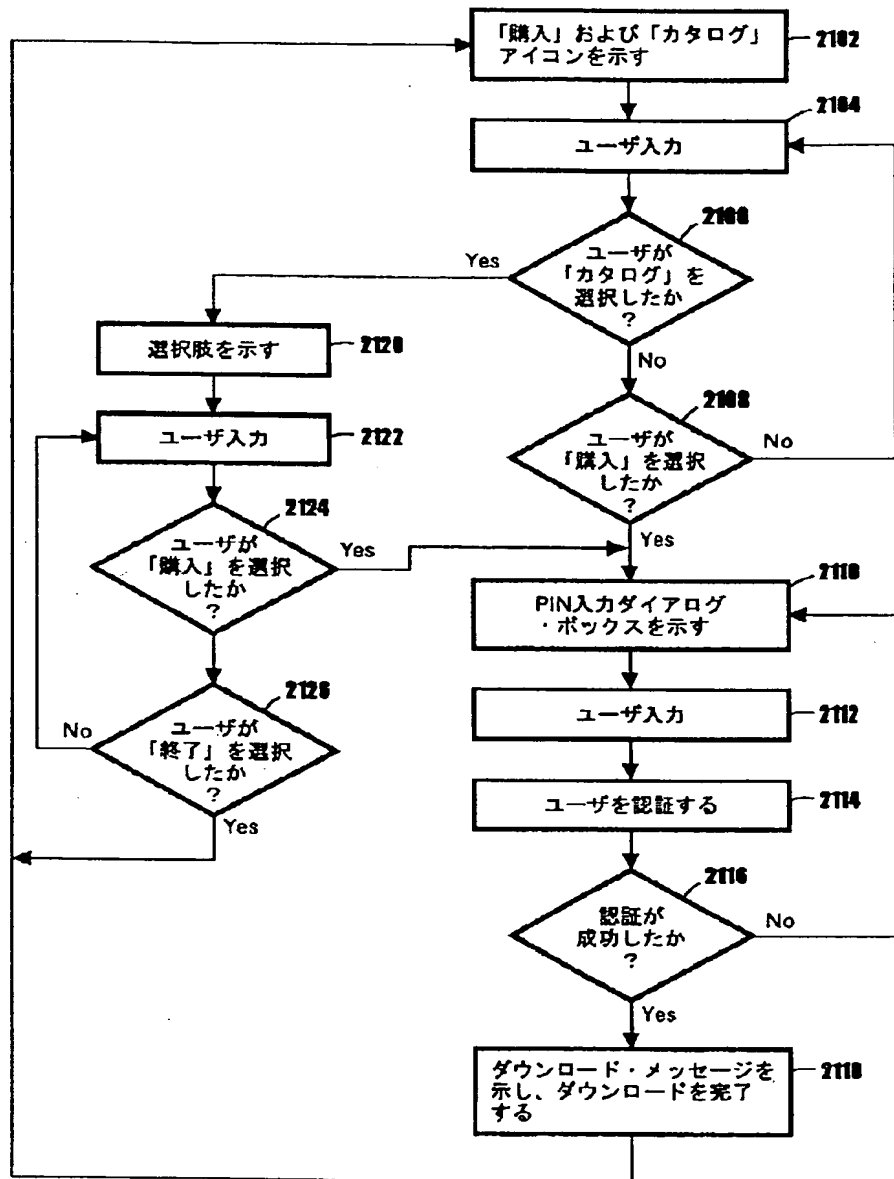


パッケージは、カルーセル方式で同報通信チャネルにより、伝送される
 カルーセルは、定期的に繰り返し現れる循環構造である
 P_1 = パッケージ #1
 P_2 = パッケージ #2
 P_N = パッケージ #N

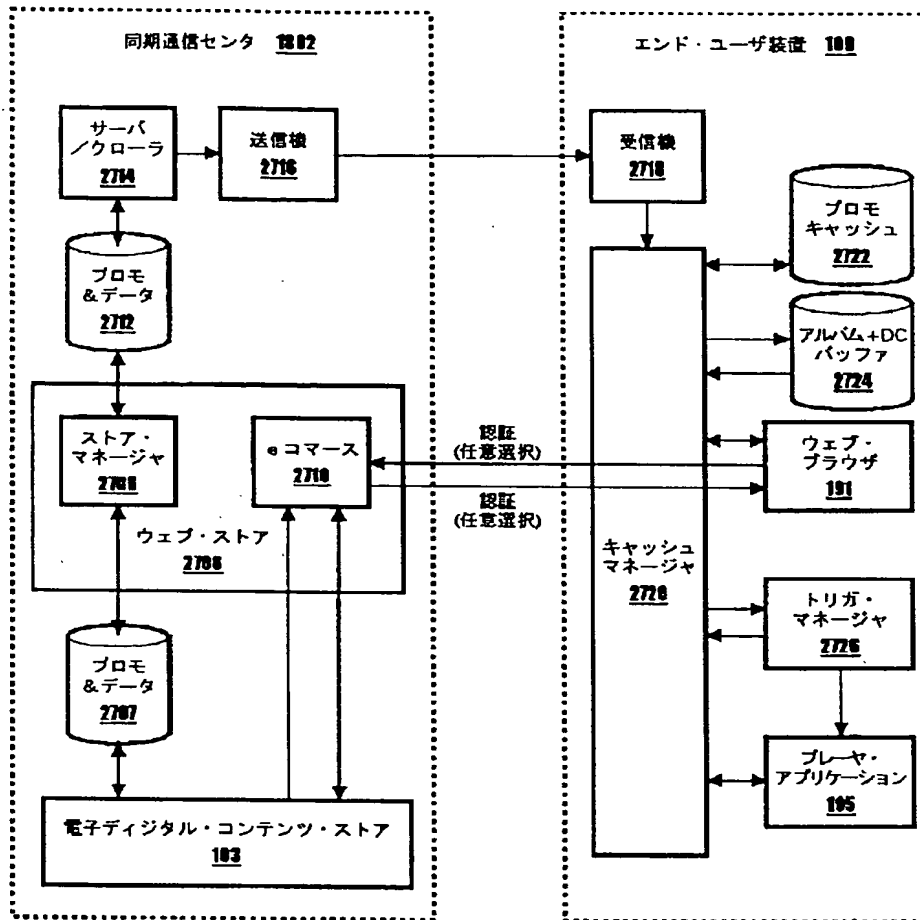
【図42】



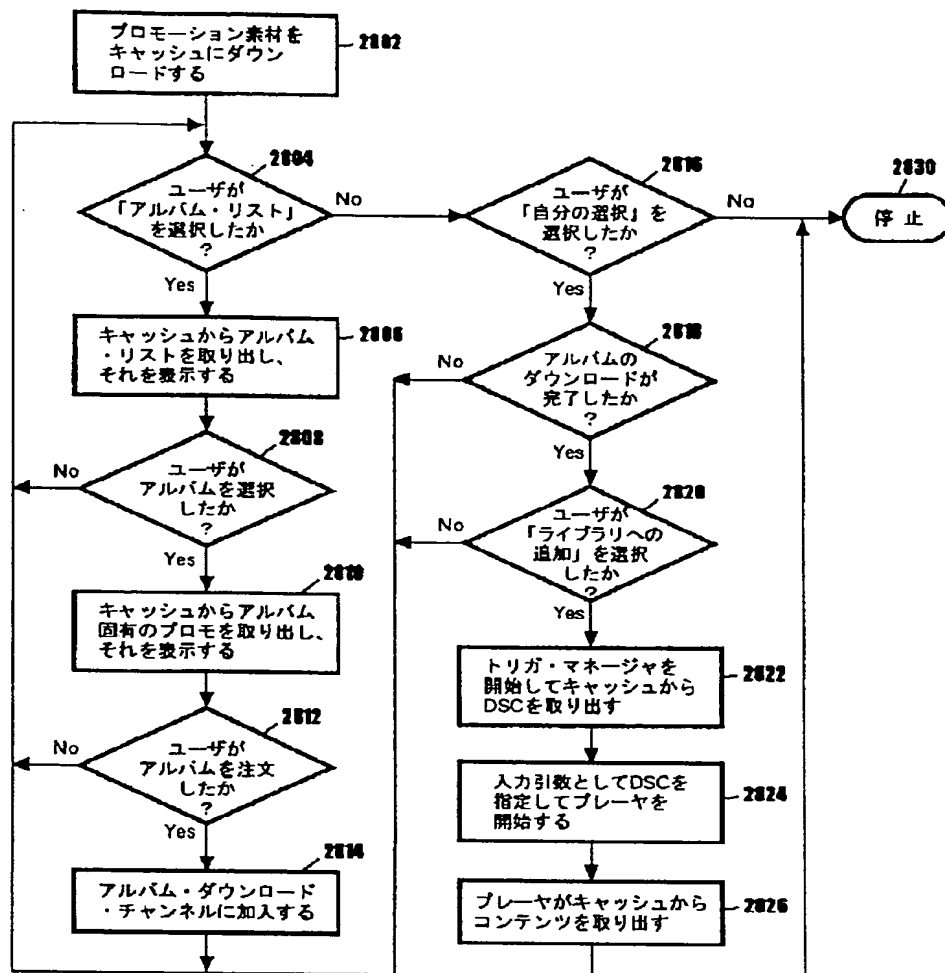
【図25】



【図31】



[図32]



フロントページの続き

(51)Int.Cl.⁷

識別記号

F I

テーマード (参考)

H 0 4 L 9/00

6 0 1 E

(72)発明者 マグダ・マウラド
アメリカ合衆国10598 ニューヨーク州ヨ
ークタウン・ハイツ チェスナット・コー
ト 397

(72)発明者 ジョナサン・ビー・マンソン
アメリカ合衆国10579 ニューヨーク州バ
トナム・ヴァレイ クレイマーズ・ボン
ド・ロード 24

(72)発明者 ジョヴァンニ・バチフィチ
アメリカ合衆国10024 ニューヨーク州ニ
ューヨーク ウェスト・エイティーズ・ファ
ースト・ストリート・ナンバ-14 101

(72)発明者 アフメド・タンタウィー
アメリカ合衆国10598 ニューヨーク州ヨ
ークタウン・ハイツ チェスナット・コー
ト 397

(72)発明者 アラー・エス・ユーセフ
アメリカ合衆国10535 ニューヨーク州ジ
ェファーソン・ヴァレイ イースト・メイ
ン・ストリート620 アpartment5デ
ィー

**This Page is Inserted by IFW Indexing and Scanning
Operations and is not part of the Official Record**

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

☐ BLACK BORDERS

☐ IMAGE CUT OFF AT TOP, BOTTOM OR SIDES

☒ FADED TEXT OR DRAWING

☒ BLURRED OR ILLEGIBLE TEXT OR DRAWING

☐ SKEWED/SLANTED IMAGES

☐ COLOR OR BLACK AND WHITE PHOTOGRAPHS

☐ GRAY SCALE DOCUMENTS

☐ LINES OR MARKS ON ORIGINAL DOCUMENT

☒ REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY

☐ OTHER: _____

IMAGES ARE BEST AVAILABLE COPY.

As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.